97

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-271011

(43)Date of publication of application : 09.10.1998

---

(51)Int.Cl. H03M 7/30
G09C 1/00
G09C 1/00

---

(21)Application number : 09-074184 (71)Applicant : SONY CORP

(22)Date of filing : 26.03.1997 (72)Inventor : MAARI KOUICHI

---

(54) DATA PROCESSING METHOD AND DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To improve the security of digital data distributed through a network.

SOLUTION: A device has a common key encryption decoding circuit 24 that decodes encrypted and compressed digital data for each processing bit number of the decoding algorithm, a buffer memory 25 that stores tentatively the decoded data in the unit of bits of a least common multiple of a processing bit number of the decoding algorithm and a processing bit number of the expansion algorithm, and an expansion circuit 26 that reads and expands the data stored in the buffer memory 25 for each processing bit of the expansion algorithm.

CLAIMS

[Claim(s)]
[Claim 1]A data processing method putting in block digital data enciphered and compressed in bitwise of the least common multiple of a processing bit number of a decryption algorithm corresponding to the above-mentioned encryption, and a processing bit number of an expansion algorithm corresponding to the above-mentioned compression, and decrypting and elongating.
[Claim 2]Digital data which was above-enciphered and was compressed is decrypted for every processing bit number of the above-mentioned decryption algorithm, The data processing method according to claim 1 saving the decrypted data concerned by bitwise of the above-mentioned least common multiple temporarily, reading data which saved [above-mentioned] for every processing bit number of the above-mentioned expansion algorithm, and elongating.
[Claim 3]A data processing device comprising:
A processing bit number of a decryption algorithm corresponding to the above-mentioned encryption for digital data enciphered and compressed.
A decoding expansion means which is put in block in bitwise of the least common multiple with a processing bit number of an expansion algorithm corresponding to the above-mentioned compression, and is decrypted and elongated.

[Claim 4]The data processing device comprising according to claim 2:
A decoding means in which the above-mentioned decoding expansion means decrypts digital data which was above-enciphered and was compressed for every processing bit number of the above-mentioned decryption algorithm.
A preserving means which saves temporarily data decrypted in the decoding means concerned at bitwise of the above-mentioned least common multiple.
An expansion means which reads data saved at the above-mentioned preserving means for every processing bit number of the above-mentioned expansion algorithm,

and is elongated.

[Claim 5]The data processing device according to claim 4 characterized by coming to allot the above-mentioned decoding expansion means in an integrated circuit.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the data processing method and device at the time of carrying out decoding extension of the digital data enciphered and compressed, for example.

[0002]

[Description of the Prior Art]Facilitate circulation of digital contents, such as a computer program, audio information, a video data, delve into a latent demand, and as a technique advantageous to a market expansion, For example, a technique like the software management method indicated to JP,6-19707,B, the software use managing system indicated to JP,6-28030,B, and the software management method indicated to JP,6-95302,B exists. The software management method indicated to above-mentioned JP,6-19707,B enables it to grasp the using state of software according to a software right holder etc. when using software, such as a computer program which is intangible property, and a video data. The software use managing system indicated to JP,6-28030,B, Use of software, such as a computer program which is intangible property, and a video data, is faced, Buy an onerous program (after buying, it can be used for free), attach a price, provide the data in which the amount of money which can be purchased is shown in the computer system, and in the case of onerous program purchase. Register with a table as a name of the available software in a same system, and. When reducing the data in which the amount of money concerned which can be purchased is shown by a software price and erasing registered software from this table, it is made to carry out renewal of an increase of the data in which the amount of money in which this purchase is possible is shown according to a situation. The software management method indicated to above-mentioned JP,6-95302,B, In order to collect a utilization charge when using software, such as a computer program which is intangible property, and a video data, according to actual utilization quantity (using frequency or utilization time) per onerous program, It is effective in the system in the case of carrying out "recording a user identification signal and a fee" with discernment of the used program, and a program right holder being able to grasp the utilization charge of a program which he

owns by collecting these records, and collecting the program utilization charges according to the utilization quantity of the program.

[0003]

[Problem(s) to be Solved by the Invention]By the way, as mentioned above, when distributing digital contents using a network, in order to stop the data volume, compression/extension art is used, and encryption/compression technology is used for anti-copying or fee collection.

[0004]That is, as shown in drawing 41, at the time of distribution of digital contents, compressing digital contents by the compression treating part 700 by the side of distribution, and carrying out encryption processing by the enciphering processing part 701 further is performed. Supposing it distributes the digital contents (compression/encryption data) generated in the distribution side like an above-mentioned example using a network, In the receiver which received the compression concerned / enciphered digital contents, decrypting the digital contents which are above-compressed and are enciphered by the decoding processing part 702, elongating in the elongation processing part 703 further, and restoring digital contents is performed. The decryption told to below is solving encryption.

[0005]In a system configuration like this drawing 41, the flow of the decryption and elongation processing in a receiver can more specifically be expressed with the flow chart of drawing 42.

[0006]In this drawing 42, as shown in step ST501, the digital contents which were above-compressed and were enciphered via the network from the distribution side are inputted into the decoding processing part 702 of the receiver of drawing 41. The data of these digital contents compressed and enciphered, By the decoding processing part 702 concerned, it is divided for every batch X bit according to the algorithm of decoding processing like step ST502, it carries out for every batch for every X bit concerned still like step ST503 based on a decode key, and is decrypted one by one. Then, in the decoding processing part 702 concerned, it is judged whether the above-mentioned decoding processing was completed about all the data of digital contents, When not having completed, it returns to step ST502 and above-mentioned processing is repeated, and when it completes, all the data of the digital contents by which decoding processing was carried out [above-mentioned] is sent to the elongation processing part 703 of the next step like step ST505.

[0007]In this elongation processing part 703, as shown in step ST506, all the data obtained by the above-mentioned extension decryption, i.e., the digital contents compressed, is divided for every batch Y bit according to the algorithm of compression elongation processing. Simultaneously, in this elongation processing part 703, elongation processing of the above-mentioned compression digital contents is carried out one by one for every batch for every Y bit concerned like step ST507. Then, in the elongation processing part 703 concerned, it is judged whether the

above-mentioned elongation processing was completed about all the data of digital contents, When not having completed, it returns to step ST505 and above-mentioned processing is repeated, and when it completes, all the data of the digital contents by which elongation processing was carried out [above-mentioned] is outputted to the latter part like step ST508.

[0008]The turn of processing of the above-mentioned encryption, compression and decryption, and extension may interchange. Namely, as shown in drawing 43, digital contents are enciphered by the encryption processing 704 by the side of distribution, When carrying out compression processing is furthermore performed by the compression treating part 705, by the receiver which received via the network, the compression[a code/]-ized digital contents concerned. Elongating the digital contents which are above-enciphered and are compressed in the elongation processing part 706, elongating by the decoding processing part 707 further, and restoring digital contents is performed.

[0009]As mentioned above, according to the Prior art, in a receiver, it is continued until processing of all the data of digital contents is completed, respectively in any [of decoding processing and elongation processing] case.

[0010]Here, the full power data of the decoding processing part 702 of the receiver of above-mentioned drawing 41 or the full power data of the elongation processing part 706 of the receiver of drawing 43 has very large data volume respectively. For this reason, before the full power data of the decoding processing part 702 of above-mentioned drawing 41 or the full power data of the elongation processing part 706 of drawing 43 is sent to the composition of the next step, respectively, it is once saved at external memory with a cheap bit unit price in many cases.

[0011]The data saved at this external memory can be taken out comparatively easily.

[0012]Therefore, it is dramatically easy for those who had bad faith, for example to rob the above-mentioned external memory of data.

[0013]Since it is easy to restore the original digital contents easily from the decrypted data concerned when the data after decrypting to external memory will be especially saved like the example of drawing 41, it is a problem that the saved data concerned is stolen.

[0014]That is, if the algorithm of the expansion system to compression is hidden like the common encryption key to the algorithm of an expansion system, respectively being opened to the public generally in many cases, what cannot perform processing of decryption does not exist. And compression digital contents after being decrypted [above-mentioned], As compared with the encryption distributed from the above-mentioned transmitting side, and the digital contents by which compression was made, it is also easy to distribute the compression digital contents which did not change in data volume, therefore were decrypted [above-mentioned] to someone else with bad faith.

[0015]When copyright etc. exist in the above-mentioned digital contents, when it above-decrypts and the above-mentioned receiver elongates the above-mentioned digital contents, it will be charged according to intention of the above-mentioned owner of a copyright etc., but. If what the theft of the digital contents after being decrypted as mentioned above is carried out happens, the danger of distributing to someone else in the place which intention of an owner of a copyright etc. does not reach, or being elongated is large.

[0016]Then, this invention is made in view of such a situation, and is a thing.

It is providing the data transmission and reception method and device which can raise the safety of the digital data distributed using the purpose.

[0017]

[Means for Solving the Problem]According to this invention, a technical problem mentioned above is solved by putting in block digital data enciphered and compressed in bitwise of the least common multiple of a processing bit number of a decryption algorithm, and a processing bit number of an expansion algorithm, and decrypting and elongating.

[0018]

[Embodiment of the Invention]Hereafter, the desirable embodiment of this invention is described, referring to drawings.

[0019]First, before giving the data processing method of this invention, the concrete contents of the device, and explanation of composition, in order to make these understanding easy, the outline composition of the whole system and the operation method of a system with which this invention is applied are briefly explained using each figure from drawing 1 to drawing 7.

[0020]The rough composition of the whole system is shown in drawing 1.

[0021]In this drawing 1, user side 200 assumes that the digital contents playback device (it will be hereafter called the player 1) and what is called a personal computer (it will be hereafter called the user terminal 50) of this invention are held.

[0022]Although the user terminal 50 is the usual personal computer, The various software which is used for this invention and which is mentioned later is stored as application software, and while, it comes to connect the loudspeaker which is the display device and sound emission means which are displaying means, a keyboard, a mouse which are information input means, etc. Via a network, the system management company 210 and connection are possible for the user terminal 50 concerned, and it has an interface means between the players 1, and data transmission and reception are possible for it.

[0023]The player 1 has composition as shown in drawing 2.

[0024]Although detailed explanation of the composition of this drawing 2 is mentioned later, The player 1 concerned as the main components of the processing route of

digital contents, It has the common key encryptosystem decoder circuit 24 which decrypts the digital contents enciphered using a contents key, the expansion circuit 26 which is the expansion means which elongate the digital contents compressed, and the D/A conversion circuit 27 which changes digital data into an analog signal at least. The decryption told to below is solving encryption.

[0025]The information which shows the right information data and the operating condition of digital contents which this player 1 uses. (These information is hereafter called point usage information) The possession money data which is needed when using digital contents, Namely, as the main components treating the billing data (it is hereafter called point information) etc. which are reduced whenever it uses digital contents, It has at least the point usage information storing memory 29 which stores the above-mentioned point usage information, and the point information storing memory 28 which stores the above-mentioned point information.

[0026]This player 1 as composition for storing the various keys used for encryption and decryption which are mentioned later The common key storage memory 22 and the key storage memory 21 for communication, It has the common code decoder circuit 24 and the open code decoder circuit 20 as composition for performing encryption and decryption using the key stored in these. This player 1 as composition relevant to the above-mentioned encryption and decryption, It also has the security ID generating circuit 19 and the timer 18 which generate the random number interlocked with the host computer of the system management company 210, and generate security ID, and the hash function circuit 25 grade which generates what is called a hash value mentioned later.

[0027]In addition, the player 1 concerned is provided with the controller 16 which is a control means which performs digital contents, various kinds of data in addition to this, and control of each component based on the program stored in ROM17, and the cell 5 as operation power at the time of carrying.

[0028]Here, as for each main components of the player 1 of drawing 2, it is desirable on security to comprise one chip of IC (integrated circuit) or LSI (large scale integration circuit). In this drawing 2, 1 chip making of each main components is carried out into the integrated circuit 10. The player 1 concerned is equipped with three terminals (the analog output terminal 2, the interface terminal 3 for PC, and the I/O terminal 4 for archive media) as an object for an interface with the exterior, and these each terminal is connected to the terminals 13, 12, and 11 in which the integrated circuit 10 corresponds, respectively. These each terminal is possible also for also unifying and newly providing another terminal, and is not scrupulous in particular.

[0029]The system management company 210 consists of the control center 211 which manages the whole system, and the store 212 which sells the above-mentioned player 1, and via the virtual online shop 230 between the user terminals 50 of user side

200, Transmission and reception of the information about supply of digital contents which is mentioned later, processing of the digital contents which compress and encipher the contents which the content provider 240 holds, the supply of digital contents processed [above-mentioned], the information transmission and reception between the financial institutions 220, etc. are performed. Between the system management company 210 and the financial institution 220, the exchange of the check of the account number of user side 200, a credit number, a name, a contact, etc., the information on the ability to trade between user side 200, etc., etc. are performed. Processing of actual price transfer etc. is performed between the financial institution 220 and user side 200. The store 212 does not necessarily need to be included in the system management company 210, and may be a sales agent.

[0030]The control center 211 of the above-mentioned system management company 210 has composition as shown, for example in drawing 3. Although detailed explanation of the composition of this drawing 3 is mentioned later, As the main components, manage digital contents and Processing treatment, such as the exhibition, encryption, and compression, The contents managing functional block 100 which has each function which is the key information used for encryption and decryption of digital contents, such as a contents key and generating of ID, Manage User Information and Encryption and decryption of correspondence (a message, point information, etc.), The user management functional block 110 provided also with the user subscription processing function part 118 which performs user subscription processing besides each function, such as generating of a confirmation message, generating of security ID, a settlement-of-accounts application between the financial institutions 230, generating of the point, etc., It has at least the usage information controlling-function block 120 which manages point usage information etc., and the controlling-function block 130 which manages the whole system and has a communication function.

[0031]An example of the actual operation method of the system constituted like drawing 1 mentioned above is explained using drawing 4 - drawing 7. The following operation methods are procedures which user side 200, the system management company 210, the financial institution 220, and content provider 240 grade actually follow.

[0032]The procedure of the purchase of the player 1 in explanation of the operation method of this system, the procedure from search of digital contents to installation of the digital contents to the memory medium for player 1, The procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for the fee collection for making the digital contents concerned usable and the procedure of distribution of the fee collection price collected from the user with appreciation of digital contents are explained in order.

[0033]First, as a procedure at the time of the purchase of the player 1, as shown in (1) of drawing 4, and (5), user side 200 actually purchases the above-mentioned player 1

from the above-mentioned store 212 by the shop front or mail order.

[0034]Personal information (a name, a contact, etc.) and settlement information (a bank account, a credit number, etc.) which were provided from above-mentioned user side 200 at the time of sale of the above-mentioned player 1 at this time as the above-mentioned store 212 was shown in (2) of drawing 4, The number (a player inherent key etc. are included) peculiar to the player 1 which sold [above-mentioned] is registered into the control center 211 of the system management company 210.

[0035]As shown in (3) of drawing 4, the control center 211 checks an account number, a credit number, etc. which were provided from above-mentioned user side 200 to the financial institution 220, and as shown in (4) of drawing 4, it acquires the information on the purport that it can trade from the financial institution 220.

[0036]User side 200 [next,] which purchased the above-mentioned player 1 as a procedure to installation of the digital contents from search of digital contents to the memory medium for player 1, Using the user terminal 50 provided with the interface means with the player 1 concerned, as shown in (1) of drawing 5, search of the digital contents of hope, selection, edit, an order, etc. are performed. Processing from the search at this time to an order is performed to the virtual online shop 230 where the user terminal 50 was connected via the network using the retrieval software stored as application software.

[0037]The virtual online shop 230 is a store which the control center 211 has provided virtually on a network, for example, and the information which shows the contents of two or more contents, for example is exhibited by this virtual online shop 230. User side 200 will place an order for desired contents based on these information provided in the virtual online shop 230. As information which shows the contents of the contents exhibited by the virtual online shop 230, When contents are video datas, such as a movie, for example, titles and advertisements, such as the movie concerned, Images, such as one scene in the movie concerned, etc. can be considered, and when contents are audio information, a track name, an artist name, the number phrase (what is called an intro) of the beginning of the music concerned, etc. can be considered. Therefore, when the above-mentioned virtual online shop 230 is accessed with the user terminal 50 of user side 200. The order of contents will be performed because the contents of two or more contents of the above-mentioned virtual online shop 230 are exhibited virtually and choose a desired thing out of these display objects on the user terminal 50 concerned.

[0038]When there are an order of digital contents, etc. from the user terminal 50 of above-mentioned user side 200, the above-mentioned virtual online shop 230 performs the supply request of digital contents to the control center 211, as shown in (2) of drawing 5.

[0039]The control center 211 which received the supply request of the digital contents concerned performs the distribution request of the digital contents which

had the above-mentioned supply request to the content provider 240. Thereby, the content provider 240 concerned supplies the digital contents which had the above-mentioned distribution request as shown in (4) of drawing 5 to the control center 211.

[0040]The control center 211 performs encryption and compression using predetermined compression technology to the digital contents rationed by the above-mentioned content provider 240, and. The virtual-online-shop name etc. which supply charge amount and contents when right holder information and the contents concerned, such as ID (content ID) of the contents concerned and an owner of a copyright of these contents, are used to user side 200 are added to these digital contents compressed and enciphered. The charge amount to contents is determined a priori by the content provider 240.

[0041]The contents processed in the above-mentioned control center 211 are sent to the virtual online shop 230, and as shown in (5) of drawing 5, as shown in (6) of drawing 5, they are further supplied to the user terminal 50 of user side 200 via this virtual online shop 230. By this, contents will be supplied to the player 1 from the above-mentioned user terminal 50, and these contents will be stored in the player 1 concerned.

[0042]It is also possible to carry out to this drawing 5 a priori about flowing to (2) - (5). That is, it not only may exhibit the information which shows the contents of two or more above-mentioned contents, but it may prepare beforehand for the virtual online shop 230 the digital contents corresponding to these exhibitions processed [above-mentioned].

[0043]Next, in the procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for the fee collection for making usable the digital contents installed in the player 1 as mentioned above. First, with the user terminal 50, shortage of the point information stored in the player 1 is checked, and a supplement demand of point information is made from the user terminal 50 concerned.

[0044]At this time, as shown in (1) of drawing 6, from the user terminal 50 concerned, the supplement request of the point information enciphered by the player 1 is transmitted to the control center 211. Simultaneously, it is read from the player 1, is enciphered and is sent to the control center 211 via the user terminal 50, a right holder's information, i.e., point usage information, corresponding to the already used digital contents, such as an owner of a copyright. Thus, transmission of point usage information was made to be performed simultaneously with the supplement request of point information, in order that user side 200 might save the time and effort which accesses the control center 211 only for transmission to the control center 211 of the point usage information concerned. Of course, it is not necessary to necessarily perform transmission of this point usage information simultaneously with the purchase

of point information, and may carry out independently.

[0045]The control center 211 which received the supplement request and point usage information of point information which were enciphered [above-mentioned] recognizes the replenishing amount of point information and the contents of point usage information which user side 200 is demanding by decoding the code concerned. The control center 211 concerned checks [of drawing 6] whether as shown in (2), the settlement of accounts for the point supplement concerned is possible to the financial institution 220. From the financial institution 220 concerned, a check accounts can be settled by investigating the account of user side 200 in the financial institution 220 will send directions of the settlement of accounts O.K. to the control center 211, as shown in (3) of drawing 6.

[0046]The control center 211 at this time connects the point usage number which will be paid to right holders, such as an owner of a copyright, to the content provider 240, i.e., the amount of money, as shown in (4) of drawing 6.

[0047]Then, in the control center 211, the letter missive of point supplementary information is enciphered, and with security ID, by making this into point supplement directions information, as shown in (5) of drawing 6, it sends to the user terminal 50. The above-mentioned point supplement directions information sent to the player 1 from this user terminal 50, It is decrypted in the player 1 concerned and supplement of the point information on the point information storing memory 28 and deletion of right holder information, including the copyright information etc. which were connected to the above place from the point usage information storing memory 29, are further performed after the check of security ID.

[0048]Next, the fee collection price collected from the user with appreciation of digital contents, That is, in the procedure of distribution of the price which will be charged directly to a user's account according to the usage information of a point, first, as shown in (1) of drawing 7, a price transfer request is made from the financial institution 220 to user side 200. When a price transfer request in particular is not made when there is sufficient balance for the account of user side 200 at this time, and there is not sufficient balance for an account, as shown in (2) of drawing 7, transfer of a price is made from user side 200 to the financial institution 220.

[0049]The financial institution 220 deducts a prescribed fee, and as shown in (3) of drawing 7, it remits the price received from user side 200 to the control center 211. That is, in the control center 211, the charge of contents processing, a financial fee, system management expense, etc. are collected from the above-mentioned price remitted from the financial institution 220. The control center 211 concerned pays the content provider 240 the royalty according to the point used previously, as shown in (4) of drawing 7, and as shown in (5) of drawing 7, it pays a store fee to the virtual online shop 230. The content provider 240 who received the above-mentioned royalty pays each owner of a copyright a royalty, and the virtual online shop 230 which

received the above-mentioned store fee pays the fee for every virtual online shop to each virtual online shop.

[0050]Thus, the price paid from user side 200, Based on said point usage information, it is distributed to a royalty, a store fee, a contents processing fee, a settlement-of-accounts fee, and a system management fee, the above-mentioned royalty -- the content provider 240 -- the above-mentioned store fee -- the above-mentioned virtual online shop 230 -- pay the system management company 210 a contents processing fee, a settlement-of-accounts fee is paid to a system management company and the financial institution 220, and a system management fee is paid to the system management company 210.

[0051]Here, in the case of the data transmission and reception between the systems of this embodiment, i.e., the data transmission and reception between the control center 211 and the player 1, in order to secure the safety of data communications, the data encryption and decryption which communicate are performed. According to this invention embodiment, it can respond as a method of encryption and decryption to both a common key encryption system and a public-key crypto system.

[0052]In the embodiment of the invention, the common key encryption system is adopted from a point of processing speed as a cipher system in the case of transmission of the variety of information of the above-mentioned digital contents, the above-mentioned point usage information, point information, a message and security ID, and others. The common keys used for encryption and decryption of these varieties of information differ corresponding to each information, respectively. The common key used for decryption of the enciphered information which is transmitted from the control center 211 in the player 1 of said drawing 2 is kept by said common key storage memory 22, Said common code decoder circuit 24 decrypts the information enciphered from the above-mentioned control center 211 using the common key currently kept in this common key storage memory 22.

[0053]The cipher system adopted by whether the player inherent key which is a peculiar key of said player 1 deals with which method as a cipher system in the case of transmission of the above-mentioned common key used for encryption and decryption of the above-mentioned variety of information on the other hand changes. That is, when the above-mentioned player inherent key supports the common key encryption system, the above-mentioned common key will be enciphered using the player inherent key concerned, and the enciphered common key concerned will be decrypted using the above-mentioned player inherent key. On the other hand, when the above-mentioned player inherent key supports the public-key crypto system, the public key of the partner point is used for encryption of the above-mentioned common key, and the secret key of the side which decrypts, respectively is used for decryption of the enciphered above-mentioned common key.

[0054]For example, in the case where the above-mentioned common key (for example,

session key mentioned later) is sent to the control center 211 from the above-mentioned player 1, When the above-mentioned player inherent key supports the common key encryption system, In the above-mentioned player 1, the above-mentioned common key encryptosystem decoder circuit 24 enciphers the above-mentioned common key using the player inherent key which the key storage memory 21 for communication is keeping, and the common key enciphered [above-mentioned] is decrypted in the control center 211 using the player inherent key which the control center 211 concerned is keeping. When the above-mentioned player inherent key similarly supports the public-key crypto system when the above-mentioned common key is sent to the control center 211 from the above-mentioned player 1 for example, The above-mentioned public-key-encryption decoder circuit 20 enciphers the above-mentioned common key in the public key of the control center 211 which the ** key storage memory 21 for communication of the above-mentioned player 1 is keeping, and the common key enciphered [above-mentioned] is decrypted in the control center 211 using the secret key which the control center 211 concerned is keeping.

[0055]On the contrary, when the above-mentioned common key (for example, contents key) is sent to the player 1, for example from the above-mentioned control center 211 and the above-mentioned player inherent key supports the common key encryption system. The above-mentioned common key is enciphered with the player inherent key which the above-mentioned control center 211 is keeping, and said common code decoder circuit 24 decrypts the common key enciphered [above-mentioned] using the player inherent key currently kept by the above-mentioned key storage memory 21 for communication in the player 1. When the above-mentioned player inherent key similarly supports the public-key crypto system when the above-mentioned common key is sent to the player 1 from the above-mentioned control center 211 for example, The above-mentioned common key is enciphered in the public key of the player 1 which the above-mentioned control center 211 is keeping, and said open code decoder circuit 20 decrypts the common key enciphered [above-mentioned] using the player inherent key, i.e., the secret key, which are kept by the above-mentioned key storage memory 21 for communication in the player 1.

[0056]The cipher system of the player inherent key itself [which was mentioned above] is determined by whether delivery (delivery to the player 1 from the system management company 210) of the player inherent key concerned is easy. That is, since the common key encryption system is more advantageous in cost, if delivery of a player inherent key is easy, a common key encryption system will be adopted, but when delivery of the player inherent key concerned is difficult, it is a high cost, but a public-key crypto system is adopted. In mounting a player inherent key in hardware and mounting a common key encryption system in software, it adopts a public-key

crypto system.

[0057]Hereafter, in an embodiment of the invention, the example which adopts the above-mentioned public-key crypto system will be given and explained in consideration of the compatibility in the case of mounting in software as a cipher system of a player inherent key itself. Namely, in the case where transmission of said common key is performed between the above-mentioned control center 211 and the player 1, When a common key (session key) is enciphered by the above-mentioned player 1 side, encryption is made using the public key of the control center 211, and the common key enciphered [above-mentioned] using the above-mentioned player inherent key (namely, secret key) is decrypted in the control center 211. On the contrary, when a common key (contents key) is enciphered by the above-mentioned control center 211 side, encryption is made in the public key of a player and the common key enciphered [above-mentioned] using the above-mentioned player inherent key (namely, secret key) is decrypted in the player 1.

[0058]Actual operation of the above-mentioned player 1, the user terminal 50, and the control center 211 which constitute the system employed using each procedure and a cipher system which were mentioned above is explained in order below.

[0059]First, it explains, referring to said drawing 2 and drawing 3 for flowing into the processing in the player 1 at the time of the point supplement, i.e., point purchase, which were mentioned above, the user terminal 50, and the control center 10 using drawing 11 from drawing 8.

[0060]The flow of the processing in the player 1 at the time of purchasing the point is shown in drawing 8.

[0061]In this drawing 8, starting of the software for point purchase beforehand installed in the user terminal 50, i.e., a personal computer, is performed by step ST1, It is waiting for the controller 16 of the player 1 in the meantime until the software for the point purchase concerned rises.

[0062]If the software for the above-mentioned point purchase rises, the controller 16 of the player 1 will receive the information inputted into the above-mentioned user terminal 50 from the user terminal 50 concerned in step ST2. An input request is made from the user terminal 50 concerned to the user who operates the above-mentioned user terminal 50 according to the software for the above-mentioned point purchase, and the information inputted into the user terminal 50 at this time is information, including a password, a point information number to purchase, etc.

[0063]The information from these user terminals 50 is received by the controller 16 via the terminal 12 of the integrated circuit 10 by which 1 chip making was carried out into the interface terminal 3 for PC of the player 1, and the player 1 concerned. The controller 16 which received the information from the user terminal 50 concerned, In step ST3, comparison with the password which the password storing memory 14 in

the integrated circuit 10 of the player 1 concerned stores, and the password in the information which received [above-mentioned] is performed, and the above-mentioned receiving password checks that it is the right.

[0064]The above-mentioned password the right and the checked controller 16, At the same time it generates the information on the purport that he would like to purchase the point in step ST4 (main point of point purchase), and a point information number to purchase and other information, Security ID is generated from the security ID generating circuit 19, and these information is made to encipher by the common code decoder circuit 24 in the following step ST5. The controller 16 reads user ID from the user ID storing memory 23 in step ST6 next, It adds to the information which enciphered [above-mentioned] the user ID concerned, and the data which added and created the user ID concerned in step ST7 is further transmitted to the user terminal 50 via the above-mentioned terminal 12 and the interface terminal 3 for PC. From this user terminal 50, the above-mentioned prepared data will be sent to the control center 211.

[0065]Since the common key encryption system is adopted as encryption of the above-mentioned prepared data at this time as mentioned above, generation of a common key is performed in advance of transmission of the prepared data concerned. For this reason, in the above-mentioned controller 16, a session key is generated as the above-mentioned common key from the security ID generating circuit 19 which is a random number generation means, for example. This common key (session key) will be sent from the player 1 to the control center 211 in advance of transmission of the above-mentioned prepared data. Since the common key concerned is that by which a code is carried out as mentioned above with a public-key crypto system here, in the above-mentioned controller 16. The public key of the control center 211 currently beforehand kept by the key storage memory 21 for communication is taken out, and it sends to the above-mentioned open code decoder circuit 20 at the same time it sends the session key which is the above-mentioned common key to the open code decoder circuit 20. Thereby by the open code decoder circuit 20 concerned, encryption of the above-mentioned common key (session key) is performed using the public key of the above-mentioned control center 211. Thus, with user ID, the enciphered session key is sent to the control center 211 in advance of transmission of the above-mentioned prepared data.

[0066]As mentioned above, when also performing transmission of point usage information with a demand of point information, the controller 16 reads point usage information including said right holder information from the point usage information storing memory 29, and these also make the above-mentioned common code decoder circuit 26 send and encipher it. This enciphered point usage information is transmitted with the above-mentioned prepared data. Simultaneously with transmission of point usage information, it is also possible to transmit the balance of point information

similarly.

[0067]Then, the controller 16 receives the data which has been sent from the control center 211 through the user terminal 50 in step ST8 and which is enciphered. The data sent from this control center 211 is the data in which the point information and information, including security ID etc., according to the above-mentioned point information number previously transmitted from the player 1 concerned to purchase were enciphered using the same common key as the above-mentioned session key.

[0068]If the data from the above-mentioned control center 211 is received, in step ST9, it sends the data concerned to the above-mentioned common code decoder circuit 24, and the controller 16 will read said common key which was generated previously and kept in the common key storage memory 22, and, similarly will send it to the common code decoder circuit 24. In the common code decoder circuit 24 concerned, the data enciphered from the above-mentioned control center 211 using the above-mentioned common key is decrypted.

[0069]Next, security ID of the data in which the above-mentioned controller 16 was decrypted [above-mentioned] in step ST10, the point information which checked by comparison with security ID from the above-mentioned security ID generating circuit 19, and was stored in the above-mentioned point information storing memory 28 in step ST11 after the check -- the above -- it corrects for the newly sent point information.

[0070]After processing of correction of the above-mentioned point information, etc. is completed, the controller 16 generates the sign of processing completion, sends it to the above-mentioned common code decoder circuit 24 with the common key read from the above-mentioned common key storage memory 22, and is made to encipher by the common code decoder circuit 24 concerned in step ST12. Then, the controller 16 transmits the sign of the enciphered processing completion concerned to the user terminal 50 via the terminals 12 and 3 in step ST13, and sends it to the control center 211.

[0071]By the above, the flow of the processing in the player 1 in the case of point purchase is completed.

[0072]Next, the flow of the processing in the user terminal 50 at the time of the above-mentioned point purchase is explained using drawing 9.

[0073]In this drawing 9, the user terminal 50 starts the software for point purchase in step ST21. When the software for point purchase concerned rises, in this user terminal 50. The input request of information, including the password mentioned above to the user who operates the user terminal 50 concerned in step ST22 according to the software for the above-mentioned point purchase, a point size to purchase, etc., is performed, If these information is inputted from a user, the inputted information concerned will be transmitted to the above-mentioned player 1 like step ST2 of said drawing 8.

[0074]Next, the user terminal 50 will transmit the data transmitted from the player 1 concerned in step ST24, if the data created like step ST7 of said drawing 8 from the above-mentioned player 1 in step ST23 is received, the address 211, i.e., the control center, which are registered beforehand.

[0075]If the user terminal 50 after performing the above-mentioned data transfer has the data return from waiting and the control center 211 in the return from the control center 211, it will transmit the data from the control center 211 concerned to the player 1 as it is in step ST25.

[0076]If the sign of processing completion is received like step ST13 of said drawing 8 from the above-mentioned player 1 in step ST26, in order to tell a user about processing of the point purchase concerned etc. having been completed, the user terminal 50 concerned, The sign of processing completion is displayed on a display in step ST27, and a user is made to check.

[0077]Then, the user terminal 50 concerned transmits the cryptogram of the sign of the processing completion sent from the above-mentioned player 1 to the control center 211.

[0078]By the above, the flow of the processing in the user terminal 50 in the case of point purchase is completed.

[0079]Next, the flow of the processing in the control center 211 at the time of point purchase is explained using drawing 10.

[0080]In this drawing 10, the control center 211 like step ST31, The data enciphered [above-mentioned] from the player 1 transmitted via the user terminal 50 by the communication function section 133 of the controlling-function block 130 by which the whole is controlled like step ST7 of said drawing 8 and step ST24 of drawing 9 in the control function part 131 is received. When this data is received, the user management functional block 110 of the control center 211, Based on the user ID attached to the received data concerned, a common key comes to hand from the database section 112 under control of the control function part 111 like step ST32, and security ID comes to hand from the security ID generating function part 116.

[0081]The common key at this time is said session key beforehand sent from said player 1, and this session key is enciphered and sent with a public-key crypto system as mentioned above. Therefore, at the time of decoding of this session key enciphered. In the user management functional block 110 of the control center 211 concerned, the secret key of the public-key crypto system of the control center 211 concerned is taken out, and the session key enciphered [above-mentioned] with this secret key is sent to a correspondence code / function decoding part 114. In a correspondence code / the function decoding part 114 concerned, decryption of a session key enciphered [above-mentioned] using the public key of the above-mentioned control center 211 is performed. Thus, the obtained session key (common key) is stored in the above-mentioned database section 112.

[0082]If the common key corresponding to the above-mentioned user ID comes to hand from the above-mentioned database section 112 and security ID comes to hand from the security ID generating function part 116, as shown in step ST33, In the correspondence code / function decoding part 114 of the user management functional block 110 of the control center 211, Further in [decrypt the data enciphered / above-mentioned / from the above-mentioned player 1 using the above-mentioned common key, and] the control function part 111, Comparison with security ID in the decrypted data concerned and security ID read from the above-mentioned security ID generating function part 116 performs content confirmation of whether to be a user with the just user side 200 (player 1) who has accessed.

[0083]In the control center 211 which checked the justification of the above-mentioned access origin. Like step ST34, by the point generating function part 113 of the user management functional block 110. The point information according to the contents of the data sent from the above-mentioned user terminal 50 is published, and the claim preparations to a user's settlement-of-accounts organization (financial institution 220) are made by the settlement-of-accounts claim function part 117.

[0084]Like step ST35, in the control function part 111, the control center 211 checks that there is no injustice in the balance and point usage information of point information from the player 1, and performs the conclusion of information for next processing. That is, a check and conclusion of whether there is any unjust use are performed from the balance of point information, and the number of the actually used point information. It is better to perform this check and conclusion desirably, although it must not carry out.

[0085]In the user management functional block 110 of the control center 211, like step ST36 after processing of above-mentioned step ST35 again, In the security ID generating function part 115, new security ID to the above-mentioned player 1 (user) is computed based on a random number generation, and above-mentioned security ID is enciphered with the above-mentioned point information in the control function part 110 further, for example. Encryption at this time is also performed using said session key (common key) sent beforehand from said player 1.

[0086]An end of the above-mentioned encryption will transmit the data which enciphered [above-mentioned] to the player 1 via the user terminal 50 under control of the control function part 131 like step ST25 of said drawing 9, and step ST8 of drawing 8 in the communication function section 133 of the controlling-function block 130 of the control center 211.

[0087]Then, in the communication function section 133 of the control center 211, like step ST38, When the processing completion sign from the user terminal 50 shown in step ST28 of said drawing 9 is received and decrypted, in the settlement-of-accounts claim function part 117 of the user management functional block 110 of the control center 211, like step ST39, The financial institution 220 is asked for settlement of

accounts based on the processing completion sign concerned. The settlement-of-accounts claim to this financial institution 220 is performed from the communication function section 132 of the controlling-function block 130.

[0088]By the above, the flow of the processing in the control center 211 in the case of point purchase is completed.

[0089]From drawing 8 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 10, and the control center 211 can be expressed, as shown in drawing 11.

[0090]That is, in this drawing 11, input, such as said password and a point size, is transmitted from the user terminal 50 to the player 1 by the input transmission T1 like step ST2 of said drawing 8, and step ST22 of drawing 9.

[0091]In the prepared data transmission T2, the data created from the player 1 by said player 1 to the user terminal 50 is transmitted like step ST7 of said drawing 8, and step ST23 of drawing 9. In data transfer T3, the data which said player 1 created from the user terminal 50 to the control center 211 is transmitted like step ST24 of said drawing 9, and step ST31 of drawing 10.

[0092]In the data transfer T4, the data enciphered from the control center 211 to the user terminal 50 in the control center 211 is transmitted like step ST37 of said drawing 10, and step ST25 of drawing 9. In the transmission T5, the data from the control center 211 is transmitted to the user terminal 50 by the player 1 as it is like step ST25 of said drawing 9, and step ST8 of drawing 8.

[0093]In the processing completion sign transmission T6, the processing completion sign from the player 1 is transmitted to the user terminal 50 like step ST13 of said drawing 8, and step ST26 of drawing 9. In processing completion sign cryptogram transmission, the processing completion sign enciphered from the player 1 is transmitted to the control center 211 like step ST28 of said drawing 9, and step ST38 of drawing 10.

[0094]Next, it explains from drawing 12 flowing into the processing in the player 1 at the time of acquisition of the digital contents mentioned above, the user terminal 50, and the control center 211 using drawing 15, referring to drawing 2 and drawing 3.

[0095]The flow of the processing in the player 1 at the time of acquisition of digital contents is shown in drawing 12.

[0096]In this drawing 12, it is waiting for the controller 16 until starting of the software for digital contents acquisition beforehand installed in the user terminal 50, i.e., a personal computer, is performed like step ST41.

[0097]If the software for the above-mentioned digital contents acquisition rises, the controller 16 will receive the data which contains digital contents from the control center 211 via the user terminal 50 like step ST42. It has at least the digital contents enciphered with the contents key (a different common key for every contents) as having mentioned above the data received via the terminals 3 and 12 from the user

terminal 50 at this time, and the content ID corresponding to the digital contents concerned. therefore, in order to use these enciphered digital contents, a contents key comes to hand from the control center 211 -- if it kicks, it will not become. The method of acquisition of this contents key is mentioned later.

[0098]The controller 16 which received the data from this user terminal 50 stores this data, i.e., the enciphered digital contents, in the memory medium connected to the I/O terminal 4 for memory media via the terminal 11 of the integrated circuit 10. Although various kinds of storages, such as a rewritable optical disc and semiconductor memory, can be considered as this memory medium, the thing in which random access is possible is desirable.

[0099]By the above, the flow of the processing in the player 1 at the time of acquisition of digital contents is completed.

[0100]Next, the flow of the processing in the user terminal 50 at the time of acquisition of digital contents is explained using drawing 13.

[0101]In this drawing 13, the user terminal 50 starts the software for digital contents acquisition in step ST51. If the software concerned rises, in this user terminal 50, the control center 211 of the address beforehand registered in step ST52 according to the software for the above-mentioned digital contents acquisition will be accessed.

[0102]At this time, the control center 211 concerned is exhibiting two or more digital contents using said virtual online shop 230. From the user terminal 50, the digital contents of the request according to the selection operation of the user out of two or more digital contents currently exhibited by this virtual online shop 230 in step ST53 are specified. That is, the user terminal 50 transmits the specification information on the contents for specifying the digital contents of the request in the digital contents exhibited by the virtual online shop 230 like step ST54 to the control center 211.

[0103]If the data which consists of data returned from the control center 211 according to the above-mentioned contents designation information, i.e., said enciphered digital contents, and content ID like step ST55 is received, The user terminal 50 concerned once stores the above-mentioned data in storing means, such as an inside, for example, a hard disk, and a memory, like step ST56.

[0104]Then, the user terminal 50 transmits the stored data (digital contents and content ID which were enciphered) concerned to the player 1 like step ST42 of said drawing 12.

[0105]By the above, the flow of the processing in the user terminal 50 at the time of acquisition of digital contents is completed.

[0106]Next, the flow of the processing in the control center 211 at the time of digital contents acquisition is explained using drawing 14.

[0107]The control center 211 shown in drawing 3 is making the virtual online shop 230 mentioned above exhibit two or more contents here. In the contents managing functional block 100 of control center 211 **, said virtual online shop 230 is generated

and, specifically, two or more above-mentioned digital contents are exhibited to this virtual online shop 230.

[0108]Thus, in the state where digital contents are exhibited to the virtual online shop 230, contents designation information is received from the user terminal 50 like step ST61 of drawing 14 step ST54 of said drawing 13.

[0109]If the above-mentioned contents designation information is received from the user terminal 50 concerned, the control function part 101 of the contents managing functional block 100 will send this contents designation information to the controlling-function block 130. The control function part 131 of the controlling-function block 130 lets the communication function section 134 for right holders pass, and transmits the contents designation information received from the above-mentioned control controlling-function block 100 to said content provider 240. Thereby from the content provider 240 concerned, the digital contents demanded in the above-mentioned contents designation information are transmitted. The digital contents which came to hand from the above-mentioned content provider 240 are sent to the contents managing functional block 100 from the controlling-function block 130, and are inputted into this contents code and compression-ized function part 104. At this time, the control function part 101 sends the contents key which is generated in a contents key and the ID generating function part 103, and is stored in the database 102 to above-mentioned contents code and compression-ized function part 104. In this contents code and compression-ized function part 104, encryption using the above-mentioned contents key is given to the above-mentioned digital contents, and further predetermined compression processing is performed. The control function part 101 adds the content ID taken out from the database 102 to the digital contents by which above encryption and compression processing were carried out, and sends it to the controlling-function block 130. As predetermined compression processing in case digital contents are audio signals, For example, like what is called ATRAC (Adaptive TRansform Acoustic Coding) that is the art currently used in what is called MD (mini disc: trademark) produced commercially in recent years, processing which carries out highly efficient compression of the audio information in consideration of human being's aural characteristic was made into an example -- it can mention.

[0110]Then, as shown in step ST62 of drawing 14, the control section 131 of the controlling-function block 130 transmits the digital contents to which it let the communication function section 133 with a user terminal pass, and it enciphered [above-] and processed [compression-], and content ID was added to the above-mentioned user terminal 50.

[0111]The flow of the processing in the control center 211 at the time of digital contents acquisition is above.

[0112]From drawing 12 mentioned above, the sequence of the information

transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 14, and the control center 211 can be expressed, as shown in drawing 15.

[0113]That is, in this drawing 15, said contents designation information is transmitted from the user terminal 50 to the control center 211 like step ST54 of said drawing 13 by the input transmission T11. In the contents transfer T12, the digital contents and content ID which were enciphered are transmitted to the user terminal 50 like step ST62 of said drawing 14 from the control center 211.

[0114]In the contents transfer T13, the digital contents and content ID which were once stored in the user terminal 50 and which were enciphered [above-mentioned] are transmitted to the player 1 like step ST57 of said drawing 13, and step ST42 of drawing 12.

[0115]Next, it explains from drawing 16 flowing into the processing in the contents key which is needed when using the digital contents mentioned above, the player 1 at the time of acquisition of the service condition and the user terminal 50, and the control center 211 using drawing 19, referring to drawing 2 and drawing 3.

[0116]The flow of the processing in the player 1 at the time of acquisition of a contents key and a service condition is shown in drawing 16.

[0117]In step ST71 of this drawing 16, in the controller 16 of the player 1, it is waiting until starting of the software the contents key beforehand installed in the user terminal 50 and for service-condition acquisition is performed.

[0118]If the above-mentioned contents key of the above-mentioned user terminal 50 and the software for service-condition acquisition rise, the information inputted into the user terminal 50 according to the software concerned will be received like step ST72 via said interface terminal 3 for PC, and the terminal 12 of the integrated circuit 10. The input supplied from the above-mentioned user terminal 50 at this time is information for requiring a contents key required to solve encryption of digital contents to appreciate. In this example, the specification information on the digital contents which use this contents key is used as demand information on the above-mentioned contents key.

[0119]The controller 16 which received this contents designation information from the above-mentioned user terminal 50, ID of the digital contents specified in the contents designation information concerned and security ID from the security ID generating circuit 19 are created, and this created data is made to encipher by the common code decoder circuit 24 in step ST73. The controller 16 adds the user ID read from the user ID storing memory 23 to the created data concerned, and transmits it to the user terminal 50 via the above-mentioned terminal 12 and the interface terminal 3 for PC. From this user terminal 50, the above-mentioned prepared data will be sent to the control center 211.

[0120]Since the common key encryption system is adopted also as encryption of the

prepared data at this time as mentioned above, in advance of transmission of the prepared data concerned, generation of a common key is performed to it. For this reason, in the above-mentioned controller 16, a session key is generated as the above-mentioned common key from the security ID generating circuit 19 which is a random number generation means, for example. This common key (session key) will be sent from the player 1 to the control center 211 in advance of transmission of the above-mentioned prepared data. Since the common key concerned is that by which a code is carried out as mentioned above with a public-key crypto system, in the above-mentioned controller 16. The public key of the control center 211 currently beforehand kept by the key storage memory 21 for communication is taken out, and it sends to the above-mentioned open code decoder circuit 20 at the same time it sends the session key which is the above-mentioned common key to the open code decoder circuit 20. Thereby by the open code decoder circuit 20 concerned, encryption of the above-mentioned common key (session key) is performed using the public key of the above-mentioned control center 211. Thus, the enciphered session key is sent to the control center 211 in advance of transmission of the above-mentioned prepared data.

[0121]Then, the controller 16 receives the enciphered data which has been sent from the control center 211 via the user terminal 50 in step ST75 so that it may mention later. The above-mentioned contents key, a service condition, security ID, etc. are enciphered as mentioning later the data sent from the control center 211 at this time.

[0122]If the data enciphered from the above-mentioned control center 211 is received, in the player 1, the data enciphered [above-mentioned] will be decrypted like step ST76, and the justification of the data will be checked. That is, the controller 16 evaluates the justification by checking security ID of the data decrypted [above-mentioned] by comparison with security ID from the above-mentioned security ID generating circuit 19.

[0123]Here, encryption is made with a public-key crypto system so that a contents key may be mentioned later, and about a service condition and security ID, encryption is made with the common key encryption system. Therefore, in order to decrypt the contents key concerned enciphered, The secret key of a public-key crypto system is required, and since the player inherent key is used as a secret key as mentioned above in the player 1 of this embodiment, the player inherent key concerned is taken out from the key storage memory 21 for communication. This player inherent key is sent to the open code decoder circuit 20 with the contents key enciphered [above-mentioned]. In this open code decoder circuit 20, the contents key enciphered [above-mentioned] is decrypted using the above-mentioned player inherent key. The contents key decrypted in this way is kept by the common key storage memory 22. On the other hand, in decrypting the service condition and security ID which are enciphered with the above-mentioned common key encryption

system, These data is sent to the above-mentioned common code decoder circuit 24, and said common key which was generated previously and kept in the common key storage memory 22 is read, and, similarly it sends to the common code decoder circuit 24. In the common code decoder circuit 24 concerned, the above-mentioned service condition and security ID are decrypted using the above-mentioned common key. The service condition decrypted in this way is stored in the point usage information storing memory 29. It is important here that the decrypted contents key and the service condition concerned are not taken out from the exterior of the player 1 concerned, the controller 16 specifically formed in the integrated circuit 10 of drawing 2 or the common key storage memory 22, and the point usage information storing memory 29 outside.

[0124]The controller 16 makes the contents key which decoded [above-mentioned] store in the above-mentioned common key storage memory 22 with the above-mentioned content ID like step ST77 after the check of this justification.

[0125]Then, the controller 16 creates the message which shows that the above-mentioned contents key came to hand in step ST78, This message is sent to the common key encryptosystem decoder circuit 24 like the above-mentioned, and said common key which was generated beforehand and kept in the common key storage memory 22 is read, and, similarly it sends to the common code decoder circuit 24. In the common code decoder circuit 24 concerned, a message is enciphered using the above-mentioned common key.

[0126]After encryption of the message concerned is completed, the controller 16 transmits this enciphered message to the user terminal 50 via the terminals 12 and 3 like step ST79. This enciphered message is made to transmit to the control center 211 after that.

[0127]By the above, the flow of the processing in the player 1 at the time of a contents key and service-condition acquisition is completed.

[0128]Next, the flow of the processing in the user terminal 50 at the time of a contents key and service-condition acquisition is explained using drawing 17.

[0129]In this drawing 17, the user terminal 50 starts the software for a contents key and service-condition acquisition in step ST81. If the designation input demand of the contents of hope is performed and specification of contents is made from a user to the user who will operate the user terminal 50 concerned in step ST82 with this user terminal 50 according to the above-mentioned software if the software concerned rises, that specification information will be generated. The user terminal 50 transmits the specification information on the above-mentioned contents to the player 1 in the above-mentioned step ST83.

[0130]Next, if the data created and transmitted by the above-mentioned player 1 like step ST74 of said drawing 16 in step ST84 is received, the user terminal 50, The data transmitted from the player 1 concerned in step ST85 is transmitted to the control

center 211 where the address is registered beforehand.

[0131]The user terminal 50 after performing a data transfer to the above-mentioned control center 211, If there is return of the data in which the contents key and service condition specified by the above-mentioned content ID from the control center 211 in waiting and step ST86, security ID, etc. were enciphered, the return from the control center 211, The data from the control center 211 concerned is transmitted to the player 1 as it is in step ST87.

[0132]The user terminal 50 after performing a data transfer to the above-mentioned player 1, The return from the player 1 in waiting and step ST88 like step ST79 of said drawing 16 from the player 1, If there is return of the message as which it was enciphered that the above-mentioned contents key came to hand, it will indicate that the above-mentioned contents key acquisition was completed to the display device connected to the user terminal 50 concerned in step ST89, and a user will be told.

[0133]Then, the message which was returned from the above-mentioned player 1 and which was enciphered [above-mentioned] is sent to the control center 211 in step ST90.

[0134]By the above, the flow of the processing in the user terminal 50 at the time of a contents key and service-condition acquisition is completed.

[0135]Next, the flow of the processing in the control center 211 at the time of a contents key and service-condition acquisition is explained using drawing 18.

[0136]In this drawing 18, the communication function section 133 with the user terminal of the control center 211, The encryption data of the content ID transmitted to the user terminal 50 from the player 1 via ** in step ST91 like step ST74 of said drawing 16 and step ST85 of drawing 17, user ID, a message, and security ID is received. This received data is sent to the user management functional block 110.

[0137]The control function part 111 of the user management functional block 110 concerned, Based on the user ID added to the encryption data which received [above-mentioned], the common key for solving the encryption concerned is taken out from the database section 112, and the above-mentioned encryption data is decoded using this common key in a correspondence code and the function decoding part 114. The control function part 111 checks the justification of the data which was received [above-mentioned] and decrypted using the user ID and security ID from the security ID generating function part 116 which were read from the database section 112.

[0138]The common key at this time is said session key beforehand sent from said player 1, and this session key is enciphered and sent with a public-key crypto system as mentioned above. Therefore, at the time of decoding of this session key enciphered. Like the above-mentioned, in the control center 211 concerned, the secret key of the public-key crypto system of the control center 211 is taken out, and the session key enciphered [above-mentioned] is decrypted using a secret key in a correspondence

code / the function decoding part 114 concerned. Thus, the obtained session key (common key) is stored in the above-mentioned database section 112.

[0139]When the justification of the data which received [above-mentioned] is checked, the control function part 111, The contents key and service condition which were specified in the above-mentioned content ID to the contents managing functional block 100 are required, The control function part 101 of the contents managing functional block 100 which received the demand concerned reads the contents key and service condition which were specified in the above-mentioned content ID from the database section 102, and transmits them to the user management functional block 110. The control function part 111 sends these contents keys and a service condition to a correspondence code / function decoding part 114 with security ID, as shown in step ST93.

[0140]Here, encryption is made with the public-key crypto system mentioned above about the contents key, and encryption is made with the common key encryption system mentioned above about a service condition and security ID. Therefore, when enciphering the contents key concerned, the public key (public key beforehand stored corresponding to the player 1) of user side 200 is taken out from said database section 112 based on the above-mentioned user ID, and it is sent to a correspondence code / function decoding part 114. In a correspondence code / the function decoding part 114 concerned, the above-mentioned contents key is enciphered using the above-mentioned public key. On the other hand, when enciphering the above-mentioned service condition and security ID, the common key (session key) specified by the above-mentioned user ID is taken out from the above-mentioned database section 112, and it is sent to a correspondence code / function decoding part 114. In the correspondence code / function decoding part 114 at this time, the above-mentioned service condition and security ID are enciphered using the above-mentioned common key.

[0141]The contents key, the service condition, and security ID which were enciphered [above-mentioned] are sent to the controlling-function block 130, and are transmitted to the user terminal 50 from the communication function section 133 with a user terminal like step ST94. The data transmitted to this user terminal 50 will be sent to the player 1 via the user terminal 50 like step ST87 of said drawing 17, and step ST75 of drawing 16.

[0142]Reception of the encryption message which the control center 211 was generated by the player 1 like step ST79 of said drawing 16, and step ST90 of drawing 17, and was transmitted via the user terminal 50 Then, waiting, When the above-mentioned communication function section 133 receives the encryption message which the above-mentioned player 1 generated like step ST95, the control center 211 concerned, Like step ST96, the encryption message concerned is decrypted with a common key, and it checks that the above-mentioned player 1 has

obtained the contents key and the service condition from the decoding message.

[0143]By the above, the flow of the processing in the control center 211 at the time of a contents key and service-condition acquisition is completed.

[0144]From drawing 16 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 18, and the control center 211 can be expressed, as shown in drawing 19.

[0145]That is, in this drawing 19, said contents designation information is transmitted from the user terminal 50 to the player 1 like step ST83 of said drawing 17 by the contents-designation-information transmission T21. In the prepared data transmission T22, the data created by the player 1 is transmitted to the user terminal 50 like above step ST74. In the prepared data transmission T23, the data created by the above-mentioned player 1 from the user terminal 50 concerned is transmitted to the control center 211. In the enciphered data sending T24, the data enciphered in the control center 211 is sent to the user terminal 50 like step ST94 of said drawing 18, and the enciphered data concerned is further sent to the player 1 by the enciphered data sending T25.

[0146]In the message transfer T26, like step ST79 of said drawing 16, In the data sending T27 as which the data which enciphered the message which shows the completion of contents key acquisition was transmitted to the user terminal 50 from the player 1, and was enciphered further, the message enciphered from the above-mentioned player 1 is sent to the control center 211 from the user terminal 50.

[0147]Next, in the player 1 which received point information, digital contents, and a contents key as mentioned above, it explains flowing into the processing at the time of actually appreciating digital contents using the user terminal 50 using drawing 20, referring to drawing 2.

[0148]Here, it is assumed that the memory medium said digital contents were remembered to be is connected to the terminal 4 of the player 1.

[0149]In this state, the digital contents which wish to appreciate from the user terminal 50 are specified to the player 1 concerned like step ST101. At this time, the specification concerned is made, when a user operates the user terminal 50, for example.

[0150]Like step ST102, according to the contents designation information from the above-mentioned user terminal 50, the controller 16 of the player 1 performs access to the above-mentioned memory medium, and reads ID of contents at this time.

[0151]Based on the content ID read in the above-mentioned memory medium, the above-mentioned controller 16 like step ST103, It accesses to said common key storage memory 22, and it checks whether the contents key is stored, and accesses to said point usage information storing memory 29, and it is checked whether the service condition is stored.

[0152]When it checks here that the above-mentioned contents key and the service condition are not stored in the above-mentioned common key storage memory 22 or the point usage information storing memory 29, the controller 16, The information on the purport that the contents key concerned etc. do not exist to the user terminal 50 is sent, and this displays the message which stimulates acquisition of the above-mentioned contents key etc. on said display device from the user terminal 50. In this case, it carries out like the flow chart for contents key acquisition mentioned above, and a contents key etc. come to hand. Thus, when a contents key etc. newly come to hand, as mentioned above in step ST104, the contents key which are enciphered is decrypted.

[0153]Next, the controller 16 checks whether there is any enough balance of the point information stored in the point information storing memory 28 based on the service condition decrypted [above-mentioned], as shown in step ST105. When the balance of the above-mentioned point information stored in the above-mentioned point information storing memory 28 is insufficient, The information on the purport that the balance of the point information concerned is insufficient is sent from the controller 16 to the user terminal 50, and, thereby, the user terminal 50 displays the message which stimulates acquisition of the above-mentioned point information on said display device. In this case, it carries out like a flow chart for point access to information which was mentioned above, and point information comes to hand.

[0154]When actually appreciating digital contents, here the controller 16, According to the digital contents concerned to appreciate, a point information number is reduced from the above-mentioned point information storing memory 28 like step ST106, Furthermore, the new point usage information according to the condition of use of the point information concerned is stored in the point usage information storing memory 29 (point usage information is updated). Thus, as point usage information newly stored to the point usage information storing memory 29, they are the right holder information corresponding to the digital contents which appreciated [above-mentioned], including owner of a copyright etc., information, other information on the reduced point information number, etc.

[0155]Then, the controller 16 will read digital contents from a memory medium, if it checks that the processing for fee collection of the cut of these point information, new storing of point usage information, etc. has been completed like step ST107.

[0156]Since the digital contents read from this memory medium are enciphered, the controller 16 transmits the digital contents enciphered [above-mentioned] to the common code decoder circuit 24 like step ST109.

[0157]In this common code decoder circuit 24, the digital contents enciphered [above-mentioned] are decrypted like step ST110 using the contents key which decrypts previously and is kept by the common key storage memory 22 based on the directions from the controller 16.

[0158]Since predetermined compression processing is made as mentioned above, these digital contents the controller 16, The digital contents by which the above-mentioned code was decrypted and by which compression processing is carried out [above-mentioned] are made to transmit to the expansion circuit 26 from the above-mentioned common code decoder circuit 24 like step ST111, and the elongation processing corresponding to the above-mentioned predetermined compression processing is made to perform here.

[0159]Then, the elongated digital contents concerned, Like step ST112, it is changed into an analog signal in the D/A conversion circuit 27, and is outputted outside (for example, user terminal 50 grade) like step ST113 via the terminal 13 of the integrated circuit 10, and the analog output terminal 2 of the player 1 concerned.

[0160]By the above, the flow of the processing in the player 1 at the time of contents appreciation is completed, and the appreciation of digital contents of a user is attained.

[0161]Next, the point usage information newly stored in the point usage information storing media 29 of said player 1 with appreciation of digital contents which were mentioned above, It explains flowing into the processing in the player 1 at the time of returning to the control center 211, the user terminal 50, and the pipe center 310 using drawing 24 from drawing 21, referring to drawing 2 and drawing 3.

[0162]The flow of the processing in the player 1 at the time of point usage information return is shown in drawing 21.

[0163]In this drawing 21, it waits for the controller 16 until starting of the software for point usage information return beforehand installed in the user terminal 50 is performed, as shown in step ST121.

[0164]If the software for the above-mentioned point usage information return of the above-mentioned user terminal 50 rises, the information inputted into the user terminal 50 according to the software concerned will be received like step ST122 via said interface terminal 3 for PC, and the terminal 12 of the integrated circuit 10. The input supplied from the above-mentioned user terminal 50 at this time is a password etc. which are entered by the user.

[0165]The controller 16 which received this contents designation information from the above-mentioned user terminal 50, The password supplied from the user terminal 50 concerned in step ST123 is compared with the password stored in the password storing memory 14, and the password concerned carries out the right check of how.

[0166]When it is checked that it is a right password in the check of the above-mentioned password, the controller 16, The balance of the point information stored in the point information storing memory 28 and the point usage information stored in the point usage information storing memory 29 are read like step ST124, respectively, and these information is enciphered.

[0167]After the balance of the above-mentioned point information and encryption of point usage information are completed, the controller 16 is attached to the data which

read user ID from the user ID storing memory 23, and enciphered [above-mentioned] like step ST125.

[0168]The data in which this user ID was attached is transmitted to the user terminal 50 via the terminal 12 and the interface terminal 3 for PC like step ST126 from the controller 16. This data is transmitted to the control center 211 after that.

[0169]As mentioned above also in the encryption at this time, the common key encryption system is adopted. That is, in advance of transmission of the data concerned, generation of a common key is performed like the above-mentioned, it is enciphered with said public-key crypto system (encryption using the public key of the control center 211), and this generated common key is sent to the control center 211 with user ID.

[0170]After transmitting data to the user terminal 50 as mentioned above, the controller 16 waits to transmit the data later mentioned from the above-mentioned control center 211 via the user terminal 50.

[0171]When the data from the above-mentioned control center 211 is received like step ST127, here in the player 1. The received data enciphered using the common key encryption system are decrypted like step ST127 using a common key like the above-mentioned, and the justification of the data is checked. That is, the controller 16 evaluates the justification by checking security ID of the data decrypted [above-mentioned] by comparison with security ID from the above-mentioned security ID generating circuit 19.

[0172]The message of the processing completion enciphered using the above-mentioned common key is also contained in the data transmitted from the above-mentioned control center 211. Therefore, the controller 16 after the check of above-mentioned security ID is completed, Send the processing completion message enciphered [above-mentioned] to the common code decoder circuit 24, the decryption using a common key is made to perform here, and it is checked that processing in the above-mentioned control center 211 has been completed by receiving this decrypted processing completion message.

[0173]By the above, the flow of the processing in the player 1 at the time of point usage information return is completed.

[0174]Next, the flow of the processing in the user terminal 50 at the time of point usage information return is explained using drawing 22.

[0175]In this drawing 22, the user terminal 50 starts the software for point usage information return in step ST131. When the software concerned rises, in this user terminal 50. If input requests, such as a password, are performed and the input of a password is made from a user to the user who operates the user terminal 50 concerned in step ST132 according to the above-mentioned software, the password will be transmitted to the player 1.

[0176]Next, if the data created and transmitted by the above-mentioned player 1 like

step ST126 of said drawing 21 in step ST133 is received, the user terminal 50, The data transmitted from the player 1 concerned in step ST134 is transmitted to the control center 211 where the address is registered beforehand.

[0177]The user terminal 50 after performing a data transfer to the above-mentioned control center 211 will transmit the data concerned to the player 1 as it is, if the data in which the return from the control center 211 is sent from the control center 211 to the player 1 in waiting and step ST135 is received.

[0178]The user terminal 50 after performing a data transfer to the above-mentioned player 1 performs the display for making a user know that processing was completed to a display device, and receives the check from a user.

[0179]By the above, the flow of the processing in the user terminal 50 at the time of point usage information return is completed.

[0180]Next, the flow of the processing in the control center 211 at the time of point usage information return is explained using drawing 23.

[0181]In the communication function section 133 with the user terminal of the control center 211, the data of the point usage information etc. which have been transmitted by step ST126 of said drawing 21 and step ST134 of drawing 22 from the player 1 via said user terminal 50 is received like step ST141.

[0182]When this data is received, the user management functional block 110 of the control center 211, The common key which is beforehand received from the database section 112 like the above-mentioned, and is stored under control of the control function part 111 like step ST142 based on the user ID attached to the received data concerned comes to hand, and security ID comes to hand.

[0183]If the common key and security ID corresponding to the above-mentioned user ID come to hand from the above-mentioned database section 112, as shown in step ST143, In the correspondence code / function decoding part 114 of the user management functional block 110 of the control center 211, Further in [decrypt the data of the point usage information etc. which were enciphered / above-mentioned / from the above-mentioned player 1 using the above-mentioned common key, and] the control function part 111, Comparison with security ID in the decrypted data concerned and security ID read from the above-mentioned database section 112 performs content confirmation of whether to be a user with the just user side 200 (player 1) who has accessed.

[0184]The data after the check of the above-mentioned justification and the contents is transmitted to the usage information controlling-function block 120. The control function part 121 of this usage information controlling-function block 120, As shown in step ST144, it is checked whether there is any injustice in use of above-mentioned user side 200 using the information stored in the database section 122 using the balance and point usage information of point information which have been sent from the above-mentioned player 1. Simultaneously, when [concerned / unjust] it comes

and things are checked, the operation which summarizes the balance and point usage information of point information in the usage information calculation function part 123 is performed.

[0185]Then, the control function part 111 of the user management functional block 110 controls the security ID generating function part 116, makes security ID compute, controls the confirmation message generating function part 115 further, and makes the message of processing completion generate, as shown in step ST145. These security ID and a processing completion message are enciphered using said common key in the correspondence code / function decoding part 114 of the user management functional block 110.

[0186]The data which was enciphered [above-mentioned] and generated will be sent to the user terminal 50 from the communication function section 133 with a user terminal, as shown in step ST146, and it will be transmitted to the player 1 from the user terminal 50 concerned like step ST135 of said drawing 22, and step ST127 of drawing 21.

[0187]By the above, the flow of the processing in the control center 211 at the time of point usage information return is completed.

[0188]From drawing 21 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 23, and the control center 211 can be expressed, as shown in drawing 24.

[0189]That is, in this drawing 24, the input of said password is transmitted from the user terminal 50 to the player 1 like step ST132 of said drawing 22 by the input transmission T31. In the prepared data transmission T32, the data which the player 1 created is transmitted to the user terminal 50 like step ST126 of said drawing 21. In the prepared data transmission T33, the data created by the above-mentioned player 1 is transmitted to the control center 211 from the above-mentioned user terminal 50 like step ST134 of said drawing 22. In the data transfer T34, the data created in the control center 211 is transmitted to the user terminal 50 like step ST146 of said drawing 23. In the data transfer T35, the data created in the control center 211 is transmitted to the player 1 via the user terminal 50 like step ST127 of said drawing 21.

[0190]Actual operation of the player 1 of the system of this embodiment, the user terminal 50, and the control center 211 serves as a flow which was mentioned above.

[0191]So far, although the flow of processing of the whole in the system of this embodiment has been explained, operation of each of the principal part of the system of this embodiment is explained in detail after this.

[0192]First, explanation about operation of the encryption and compression in this invention embodiment, and extension and decryption is given.

[0193]Like the system of an embodiment mentioned above, when distributing digital contents using a network, in order to stop the data volume, compression/extension

art is used, and encryption/compression technology is used for anti-copying or fee collection. That is, compressing digital contents and carrying out encryption processing further by the distribution side (an above-mentioned example the control center 211 side), is performed. When distributing the digital contents (encryption/compressed data) generated at the transmitting side (control center 211 side) like an above-mentioned example using a network, In a receiver (an above-mentioned example player 1), decrypting, after receiving the digital contents which were above-enciphered and were compressed, elongating further, and restoring digital contents is performed. The turn of processing of the above-mentioned encryption, compression and decryption, and extension may interchange.

[0194]When copyright etc. exist in the above-mentioned digital contents, when the above-mentioned receiver elongates the above-mentioned digital contents with the above-mentioned decryption, it will be charged according to intention of the above-mentioned owner of a copyright etc. Although this fee collection is performed by mainly purchasing, the key, i.e., the contents key, of decryption, it is in the method of purchasing this contents key variously.

[0195]Here, as mentioned above, when procedure which compresses digital contents, is enciphered, is decrypted and is elongated is followed, the user who had bad faith, for example can obtain comparatively easily the compressed data decrypted [above-mentioned]. Namely, the compressed data of digital contents, Generally capacity is large, therefore For example, since not an internal memory but the ** value of a common contents playback device of a receiver are accumulated in external memory in many cases, It is because it is easy to take out unjustly the digital contents compressed [above-mentioned] by the connection section with direct or external memory from this external memory.

[0196]What cannot be processed if the algorithm of the expansion system to compression is hidden like the key of a code general to the algorithm of an expansion system, respectively being opened to the public in many cases does not exist. And as compared with the digital contents by which the encryption distributed from the above-mentioned transmitting side and compression were made, **** which distributes the compression digital contents which did not change in data volume, therefore were decrypted [above-mentioned] with bad faith is also easy for the compression digital contents decrypted [above-mentioned]. Namely, according to the method which is enciphered and distributes digital contents after compressing [above-mentioned]. The danger that the compression digital contents which can elongate anyone easily will be distributed further in the place which a theft is easily carried out to a user with bad faith, and intention of an owner of a copyright etc. does not reach for this reason, or will be elongated is large.

[0197]So, in the embodiment of the invention, in order to make it possible to raise the safety of the digital contents distributed using a network in view of such a situation, in

the player 1 of above-mentioned drawing 2, processing as shown in the flow chart of the following drawing 25 is performed.

[0198]Namely, in the decoding processing in the common code decoder circuit 24 of the player 1 of drawing 2, and the elongation processing in the above-mentioned expansion circuit 26. The data of the digital contents by which compression processing was carried out with the encryption read from said memory medium like step ST151, First, it divides into the unit of the least common multiple lcm (X, Y) of the batch X bit of the algorithm of decoding processing, and the algorithm batch Y bit of elongation processing.

[0199]Next, as the data of digital contents in which the above-mentioned encryption divided into the unit of the above-mentioned least common multiple lcm (X, Y) and compression processing are made is shown in step ST152, decoding processing is performed by the above-mentioned common code decoder circuit 24 for every unit of the least common multiple lcm (X, Y) concerned.

[0200]As the data of digital contents in which the unit of the least common multiple lcm (X, Y) obtained by the decoding processing concerned is compressed is shown in step ST154, elongation processing is performed to all the compressed data for the unit concerned in the above-mentioned expansion circuit 26.

[0201]Then, the decryption and elongation processing for every unit of this least common multiple lcm (X, Y) are continued until the processing about all the data of digital contents by which compression processing was carried out with the above-mentioned encryption is completed. . Namely, judgment whether the decryption and elongation processing for every unit of the least common multiple lcm (X, Y) were completed to all the data of digital contents should do to be shown in step ST155. When not having completed and it returned and completes to step ST152, the flow chart of the processing concerned is completed.

[0202]The digital contents by which all the data was decrypted and elongated by this will be obtained.

[0203]Although the decoding data of the above-mentioned least-common-multiple lcm (X, Y) unit will exist, the data volume of the decoding data concerned also has little processing of the flow chart of drawing 25 in the player 1 concerned. For this reason, a possibility of being stolen like [in the case of saving at external memory which can be saved at an internal memory with high safety even if comparatively expensive, therefore was mentioned above] will become very low.

[0204]In the above-mentioned player 1 in this embodiment, the buffer memory 25 of drawing 2 is formed as an internal memory for securing the above-mentioned safety between the above-mentioned common code decoder circuit 24 and the expansion circuit 26. That is, this buffer memory 25 is formed in the integrated circuit 10 of one chip, and it is hard to be accessed from the outside, therefore data is not taken out outside.

[0205]In an above-mentioned flow chart, are made to perform decryption and elongation processing to all the data for the unit of the least common multiple lcm (X, Y), and as concrete composition for it, For example, the data of digital contents is first divided into the batch X bit of the algorithm of decoding processing like composition of being shown in drawing 26, By performing decoding processing to the data of this X bit, gathering the data in which the X bit concerned by which decoding processing was carried out is compressed after that by the algorithm batch Y bit of elongation processing, and elongating the compressed data of the Y bit concerned. It is made to realize the decryption and elongation processing in the unit of the least common multiple lcm (X, Y) as mentioned above.

[0206]The common code decoder circuit 24 of the player 1 which realizes this consists of the input part 30 and the code decoding part 31, and the above-mentioned expansion circuit 26 consists of the expanding part 32 and the outputting part 33. Said buffer memory 25 is formed between these common code decoder circuit 24 and the expansion circuit 26.

[0207]If encryption processing to the above-mentioned digital contents is performed as a more concrete example here for example, using the DES (Data Encription Standard) code, The encryption processing concerned and decoding processing corresponding to it will be performed by 64 bitwises.

[0208]In the case of the elongation processing to the compressed digital contents, it changes also with the compression ratios and sampling frequencies, but under the present circumstances, it is processed per 1K - 2 K bits/channel in many cases. Here, it is assumed that it is processed for every 1.28K bit for convenience.

[0209]Therefore, in the case of the system using the above-mentioned DES cipher system and the compression expansion system for every above-mentioned 1.28K bit, the above-mentioned least common multiple lcm is set to 1.28K.

[0210]Said digital contents enciphered and compressed are inputted into the input part 30 of the basis of such conditions, and the common code decoder circuit 24 of drawing 26. In the input part 31 concerned, the digital contents which were enciphered [above-mentioned] and compressed are divided into [every batch X bit of the algorithm of the above-mentioned decoding processing], i.e., 64 bits, data, and are outputted to the code decoding part 31.

[0211]In this code decoding part 32, decoding processing of the above-mentioned X bit, i.e., 64 bits, data is carried out concerned every 64 bits. The 64 bits [which was obtained by the decryption in this every 64 bits] data compressed is sent to the buffer memory 25.

[0212]When the compressed data for the algorithm batch Y bit of elongation processing, i.e., a 1.28K bit, accumulates according to the directions from said controller 16, the buffer memory 25 concerned, The compressed data for the 1.28K bit concerned is outputted collectively, and this compressed data is sent to the

expanding part 32 of the above-mentioned expansion circuit 26.

[0213]The above-mentioned expanding part 26 elongates the compressed data for the 1.28K bit inputted [above-mentioned], and outputs it to the outputting part 33.

[0214]The controller 16 controls processing of the decoding section 31, and processing of the expanding part 32, monitoring the data volume which accumulated in the buffer memory 25.

[0215]If 20 pieces (= 1280/64) are parallel in decoding processing if it is this case, and it processes, it will become a more nearly high-speed processing system.

[0216]In addition, when performing not hardware constitutions like said drawing 2 or drawing 26 but processing mentioned above with the programmable device, the controller 16 will process based on a decoded program or an extension program, corresponding to the situation of the buffer memory 25.

[0217]Although the digital contents enciphered after compressing were supplied to the player 1 and the example elongated after decrypting these digital contents compressed and enciphered was given by the player 1 by above-mentioned explanation, Even if it is a case where the compressed digital contents are elongated and decrypted after enciphering, the same effect as **** can be acquired.

[0218]The algorithm of compression / extension, and encryption/decryption is not limited, and this invention is effective to any methods.

[0219]Thus, according to this invention, the safety of the digital contents distributed using a network improves.

[0220]Next, explanation about generating operation of said security ID is given.

[0221]As point information comes to hand beforehand and being mentioned above like this embodiment in the case of a method which reduces the point information concerned according to appreciation of digital contents, After the control center 211 on a network performs checks as arbitrary after receiving communication of a purchase request of the point information from the user terminal 50 of user side 200 as financial institution 220 and others, it enciphers the point information and sends it to the player 1 of user side 200 via a network.

[0222]In the case of a method which obtains point information beforehand and reduces the point information concerned like this embodiment according to appreciation of digital contents, between the control center 211 and the player 1 (user terminal 50), an exchange of the data same each time as the degree of the purchase of point information -- carrying out (for example, the information of "the point information on 3000 cyclotomies" corresponding to "3000 supplement demand of the point information on a cyclotomy" and it which were enciphered is exchanged) -- it is based on those who have bad faith, for example. The amount-of-money supplement depended for what is called "impersonating" to the financial institution 220 serves as a problem. "Impersonating" to the financial institution which says here means what a person with the above-mentioned bad faith impersonates an original user (this

embodiment user side 200), and obtains point information unjustly.

[0223]Namely, if the data same each time as the degree of the purchase of point information is exchanged, For example, a person with bad faith robs a communication line of the data concerned, and the same data is generated, In the case as the destination is made into itself (person with bad faith) to the control center 211 and acquisition of point information was requested. A person with the bad faith concerned can obtain point information, and the claim of the purchase price of this point information has further a possibility that the problem that it will be made by original user side 200 may occur.

[0224]Then, in order to prevent such injustice, in the system of this invention embodiment, the random number generated by the random number generation function which has interlocked beforehand by both a receiver (player 1 side) and the distribution side (control center 211 side) is used for the improvement in safety. According to this embodiment, said security ID is generated as the above-mentioned random number. What is necessary is to initialize the timer 18, for example and just to synchronize operation between both, for example in the cases, such as a user's registration procedure, in order to interlock a random number generation among both.

[0225]That is, the operation at the time of the player 1, for example, point access to information, from the control center 211 at the time of using this random number (security ID) serves as the following flows.

[0226]The data sent from the control center 211 to the player 1 is made with the data which consists of security ID generated [above-mentioned] with the point information enciphered using the common key (session key) which came to hand beforehand from the player 1 as mentioned above at the time of the purchase of point information.

[0227]The controller 16 of the player 1 is sent to the common code decoder circuit 24, as the data received from the control center 211 concerned was mentioned above, and it performs decoding processing here using said common key. By this, the point information and security ID which have been sent from the control center 211 will be obtained.

[0228]Then, the controller 16 of the player 1 compares security ID sent from the above-mentioned control center 211 with security ID generated in the own security ID generating circuit 19. In this comparison, the controller 16 stores in said point information storing memory 28 the point information sent from the above-mentioned control center 211, only when security ID from the control center 211 and security ID which the above itself generated are in agreement.

[0229]By this, only the player 1 of valid-user side 200 can obtain point information. the malicious person who in other words has the player 1 of valid-user side 200, and the same player -- said -- impersonating, even if it is going to obtain point information unjustly, Since security ID of the player which the person of the bad faith concerned

has, and security ID sent from the above-mentioned control center 211 are not in agreement, the person with this bad faith will not get said inaccurate point access to information depended for impersonating.

[0230]Of course, security ID generated in the player 1 of user side 200, The security ID generating circuit 19 provided in the integrated circuit 10 of the player 1 concerned occurs, and since it is what cannot be taken out outside, a person with bad faith cannot steal the security ID concerned.

[0231]Although some are various in the composition which generates the random number as above-mentioned security ID, the example is shown in drawing 27. The composition of this drawing 27 is one example of the security ID generating circuit 19 of said drawing 2.

[0232]In this drawing 27, the one-way function generating part 40 generates what is called a one-way nature function. The inverse function is far difficult for calculation with a function with the above-mentioned one-way nature function comparatively easy to calculate. It receives by secret communication etc. beforehand and this one-way function can also be saved at the one-way function generating part 40 concerned. The one-way function generating part 40 can also be made to generate the above-mentioned one-way function by making into an input function the hour entry from the timer 18 established in the integrated circuit 10 of said drawing 2. The above-mentioned one-way function is sent to the random number deciding part 43.

[0233]The number generating part 41 of users generates the predetermined number of users defined for every user. This number of users is beforehand sent by secret communication etc., and is saved at the number generating part 41 of users concerned. The user ID which said user ID storing memory 23 stores, for example can also be used for this number of users.

[0234]The random number database 42 stores a random number, and stores 99 random numbers.

[0235]The time communication storage parts store 44 memorizes the time communication information sent, for example from the controller 16. This time communication information is information which shows the time communication between the player 1 and the control center 211.

[0236]These one-way functions, the number of users, and time communication information are sent to the random number deciding part 43. The random number deciding part 43 concerned generates the random number of the range beforehand memorized by the random number database section 42 from the above-mentioned one-way function and the number of users, for example based on the hour entry from said timer 18 (for example, 99 pieces).

[0237]Namely, if the above-mentioned time communication information is the communication which is the 1st time in this random number deciding part 43, The 99th random number is taken out from the above-mentioned random number database

section 42, and if for example, time communication information is the communication which is the n-th time, the 100-n-th random numbers will be picked out from the above-mentioned random number database 42, and this taken-out random number is outputted as said security ID.

[0238]The composition of this security ID generating has the same thing in the player 1 and the control center 211.

[0239]When finishing using all the random numbers stored in the random number database section 42, In the above-mentioned random number deciding part 42, 100 pieces - the 199th random number are calculated, or secret communication of a new random number and unidirectional function is carried out, and it re-stores in the random number database section 42, or, on the other hand, reconstructs to the tropism function generation part 40.

[0240]Although a random number (security ID) is generated and he is trying to improve the safety for every communication in the explanation mentioned above, According to this embodiment, since he is also trying to generate programmably a common key (session key) different each time whenever it communicates between user side 200 and the control center 211 side as mentioned above, safety is improved further.

[0241]Here, the above-mentioned random number is inserted about the transmission sentences (for example, message etc.) actually transmitted, and signs that encryption by a session key is made, and signs that a random number is taken out from a receiving sentence and the check of justification is made are explained using drawing 28 and drawing 29. He is also trying to add a signature (digital signature) to a transmission sentence in the example of these drawing 28 and drawing 29.

[0242]In this drawing 28, first, as a flow which enciphers said common key with a public-key crypto system, and transmits, it generates as a common key which uses said session key for communication, and this common key is enciphered by the public key of a receiver to the public-key-encryption chemically-modified degree P8 by the common key generating process P7 for communication. This enciphered common key is sent to a receiver.

[0243]On the other hand, as a flow in the case of enciphering the message as a transmission sentence with a common key encryption system, and transmitting, in the message generation distance P1, the message M is generated and a random number (said security ID) is generated at the random number generation process P5, for example. These messages M and a random number are sent to the common key encryptosystem chemically-modified degree P6. In the common key encryptosystem chemically-modified [this] degree P6, the above-mentioned message M and a random number are enciphered using the common key by which it was generated at the above-mentioned common key generating process P7 for communication.

[0244]When adding the above-mentioned digital signature, the above-mentioned

message M is sent to the hash value calculation process P2. In the hash value calculation process P2 concerned, what is called a hash value is calculated from the above-mentioned message M. A hash value is address information called for by a hash method, and a hash method performs a predetermined operation to some contents (keyword) of data (in this case, the message M), and uses that result for it as an address. The hash value (M) generated from this message is sent to the secret key cryptosystem chemically-modified degree P4 as a digital signature. In the secret key cryptosystem chemically-modified [this] degree P4, the above-mentioned digital signature is enciphered with the secret key of the transmitting side. This enciphered digital signature is sent to the common key encryptosystem chemically-modified degree P6. This enciphers the above-mentioned digital signature in the common key encryptosystem chemically-modified degree P6 using the common key by which it was generated at the above-mentioned common key generating process P7 for communication.

[0245]These messages M, a digital signature, and a random number are transmitted to a receiver.

[0246]Next, the flow of processing by the receiver corresponding to drawing 28 is explained using drawing 29.

[0247]In this drawing 29, the common key transmitted from the above-mentioned transmitting side is first decrypted with the secret key of the receiver concerned at the secret key decryption process P11 as a flow which decrypts said common key with a public-key crypto system.

[0248]At the common key decoding process 13, the message M transmitted [above-mentioned] is decrypted using the common key decrypted at the above-mentioned secret key decryption process P11 as a flow which, on the other hand, decrypts the message M enciphered with said common key encryption system. This decrypted message M will be sent to other processes by the other functional transmission processes P20.

[0249]The hash value which decodes a digital signature and which flowed and was decrypted at the above-mentioned common key decryption process P13 is decrypted using the public key of the transmitting side at the public key decryption process P14. Simultaneously, in the hash value calculation process P17, a hash value is calculated from the above-mentioned message M. The check of the hash value decrypted by these public key decryption process P14 and the hash value calculated by the above-mentioned hash value calculation process P17 being compared, and not being altered by the comparison process P19, is performed.

[0250]About the transmitted random number, the random number decrypted at the above-mentioned common key decryption process P13 and the random number generated at the random number generation process P21 of the receiver concerned are compared by the just exact private seal process P22, and the check of

justification is performed.

[0251]By the way, in the system of this embodiment shown in drawing 1 mentioned above, the system management company 210, the virtual online shop 230, and the content provider 240 are formed as a system side to user side 200. The financial institution 220 of drawing 1 is an external bank etc., for example.

[0252]The control center 210 of the above-mentioned system management company 210, Exhibition of digital contents and management of distribution in the virtual online shop 230, between the financial institutions 220 -- the main work by the side of systems, such as collection of the accounting information of user side 200, or a variety of information, distribution and those managements, encryption of the digital contents from the content provider 240, and a security management of the information to treat, -- all are performed mostly.

[0253]However, in the system which distributes digital contents using a network which was mentioned above, In the time of the user side obtaining digital contents from the system side, and the case of the fee collection accompanying use of digital contents, communication will concentrate on the system side and there is a possibility that a satisfying response may no longer be obtained to the user side.

[0254]So, in other embodiments of this invention, it makes it possible to prevent concentration of communication which was mentioned above and to raise a communicative response by the function of the system management company 210, and more specifically dividing the function of the control center 211 as follows.

[0255]Namely, the content exhibiting distributing institution 310 which has a function which exhibits digital contents and distributes the composition by the side of the system to user side 200 in other embodiments of this invention as shown in drawing 30, Accounting information control machine Seki 320 which has the function to manage the accounting information of the user of a fixed area, It divides into the data generation of enciphering digital contents, distribution of generated data to the above-mentioned content exhibiting distributing institution 310, the information gathering from above-mentioned accounting information control machine Seki 320, division of earnings, and the system management organization 330 that has the function to perform the security management and others of the whole system, User side 200 and communication are independently attained for each organization 310,320,330, respectively.

[0256]In composition like this drawing 30, the content exhibiting distributing institution 310 is scattered on the network in the world, two or more arrangement is possible for it, and if even communication charges are paid, it can access user side 200 to the content exhibiting distributing institution 310 of every area. For example, when user side 200 wants for digital contents to come to hand, the above-mentioned content exhibiting distributing institution 310 is accessed from user side 200, and digital contents come to hand. Digital contents [which were enciphered by the system

management organization 330], i.e., user, side 200 will be the digital contents at this time in the state which can be transmitted directly using a network.

[0257]Holding not much many users installs accounting information control machine Seki 320 for a moderate number of every users undesirably therefore on safety management in order to treat accounting information. However, since the attack point (accounting information control machine Seki 320) from the 3rd person with bad faith will be increased and it will be traded off if it installs not much mostly, optimizing is desirable. For example, when user side 200 performs communication about fee collection, it accesses from user side 200 to above-mentioned accounting information control machine Seki 320.

[0258]The above-mentioned system management organization 330 Subscription to a user's system, and registration of means of settlement, Profits distribution to the profits beneficiary of the collection of money from a user, said right holder, the content exhibiting distributing institution 310, and accounting information control machine Seki 320 grade, etc. raise security by carrying out by summarizing management of important information on security. However, as for the system management organization 330 concerned, it is desirable not to necessarily establish one place in the world and to install in a certain settled unit, for example, the unit of a country etc. For example, when user side 200 performs important communication on [, such as subscription to this system, and registration of means of settlement,] security, it carries out by accessing from user side 200 to the above-mentioned system management organization 330. The system management organization 330 concerned which obtained information performs profits distribution to the collection of money and the profits beneficiary from the user concerned collectively from above-mentioned accounting information control machine Seki 320. It is supplied to the system management organization 330 concerned, the source data, i.e., the contents, which an owner of a copyright etc. have, they are changed into the digital contents by which encryption etc. were made here, and are distributed to the above-mentioned content exhibiting distributing institution 310.

[0259]As mentioned above, by distributing the function by the side of a system to the three organizations 310,320,330, and making direct access of it possible between user side 200 and each organization 310,320,330, communicative concentration is prevented and it becomes possible to raise a communicative response. According to the content exhibiting distributing institution 310, it can respond also to a thing like what is called an existing virtual Mall, and it is effective also in sales promotion and attractive for a user. By dividing accounting information control machine Seki 320 independently, it is useful for the dishonesty prevention which conspired with exhibition and the selling function of contents. In order that a fixed number may obstruct the user who manages, the controlling function who receives unjustly is also more effective.

[0260]In the system of other embodiments of this invention shown in drawing 30 mentioned above below, It explains that the accounting information accompanying the information flow at the time of acquisition of the contents key subscription to a user's system, the purchase of point information, and for decoding of the enciphered digital contents, etc., the flow in the case of circulation of the information for contents and contents appreciation, and use of contents flows.

[0261]First, the principal part of the flow of the time of subscription to a user's system is explained using drawing 31.

[0262]In the case of the subscription registration to a user's system, the following procedures depended on the user subscription support functional block 402 of the system management organization 330 follow, and registering operation is performed at it.

[0263]From user side 200 [1], i.e., said player, and the user terminal 50, the information which shows the intention of subscription to a system is first sent via a network like the subscription intention sending T41 to the system management organization 330. The information on the above-mentioned subscription intention of having been inputted into the communication function block 401 of the system management organization 330 is sent to the user subscription support functional block 402.

[0264]Reception of the above-mentioned subscription intention information of the user subscription support functional block 402 concerned will send the information on a file required for subscription to user side 200 via the communication function block 401 like the subscription required file sending T42.

[0265]In user side 200, creation of the subscription request according to a predetermined format is performed based on the subscription required file sent from the above-mentioned system management organization 330. The drawn-up subscription request concerned is sent to the system management organization 330 like the subscription request sending T43.

[0266]The user subscription support functional block 402 which received the above-mentioned subscription request sends the information which explains the function of a client to user side 200 like the client function sending T44.

[0267]From user side who received information on client function concerned 200, User Information, such as users' information, for example, an account number and a credit number which were mentioned above, a name, and a contact, is sent to the system management organization 330 like the User Information sending T45.

[0268]The user subscription support functional block 402 which received sending of the User Information concerned notifies the information on the purport that the registration procedure of subscription was completed to user side 200 like the registration procedure completion notification T46.

[0269]The user subscription support functional block 402 of the system management

organization 330 transmits User Information to accounting information control machine Seki 320 via the communication function block 401 like the User Information sending T47 after the completion of procedure of this user subscription registration. Accounting information control machine Seki 320 which received this User Information saves the User Information concerned at the database function block 367.

[0270]By the above, the main flows of the time of subscription to a user's system are completed. The explanation about other composition currently mentioned to this drawing 31 is mentioned later.

[0271]Next, the principal part of the flow of the information at the time of acquisition of the key the purchase of point information and for decoding of the enciphered digital contents, etc. is explained using drawing 32. Since the information on the contents key the purchase of the above-mentioned point information and for decoding of the enciphered digital contents is information for using contents, it is made to simplify these and to call it royalty information by the following explanation.

[0272]When a user obtains the important information (here royalty of contents) used by a system, access is made from user side 200 to accounting information control machine Seki 320 where the assignment in its duty is beforehand made for every user side 200. To access of an acquisition demand of the contents royalty information sent from above-mentioned user side 200, the royalty issuing function block 362 of accounting information control machine Seki 320 corresponds, and issue of a royalty is performed according to the following procedures.

[0273]First, from user side 200, the information on the purport that he would like to purchase a royalty is sent to accounting information control machine Seki 320 like the purchase written request sending T51. The information on the purport that he would like to purchase a royalty is information on the purchase written request which followed the predetermined format by user side 200. Thus, the information on the above-mentioned purchase written request inputted into the communication function block 361 of this accounting information control machine Seki 320 is sent to the royalty issuing function block 362 via a network.

[0274]In the royalty issuing function block 362 concerned, if the information on the above-mentioned purchase written request is received, it will carry out based on User Information saved at the database function block 367, the information on a new royalty will be generated, and the information on the royalty concerned will be sent to user side 200 like the new royalty sending T52.

[0275]If the receipt of the information on the above-mentioned new royalty is checked, user side 200 will draw up the receipt written confirmation according to a predetermined format, and will send it to the royalty issuing function block 362 of accounting information control machine Seki 320 like the receipt written confirmation sending T53.

[0276]By the above, the main flows of the time of the purchase of a royalty are

completed. The explanation about other composition currently mentioned to this drawing 32 is mentioned later.

[0277]Next, the principal part of the flow in the case of circulation of the information for contents and contents appreciation (here, they are a service condition and a contents key) is explained using drawing 33.

[0278]First, the contents acquisition functional block 342 of the content exhibiting distributing institution 310 charges digital contents to the system management organization 330 like the contents bill sending T62.

[0279]In the contents distribution functional block 404, the system management organization 330 which received the contents bill concerned is processed so that the demanded contents can be circulated. That is, in this contents distribution functional block 404, the digital contents (enciphered digital contents) of the state which can be sent to user side 200 are generated. These processed digital contents are sent to the content exhibiting distributing institution 310 like the contents sending 63.

[0280]In the content exhibiting distributing institution 310 concerned, the digital contents processed [above-mentioned] are saved at the contents database functional block 345.

[0281]In the contents distribution functional block 404 of the system management organization 330. The contents key for decoding the contents enciphered as content ID and a service condition as information for contents appreciation is sent to accounting information control machine Seki 320 like the information sending T64 for contents appreciation.

[0282]In accounting information control machine Seki 320, a contents key and the service-condition receipt functional block 363 receive the information for the above-mentioned contents appreciation, and it is saved at the database function block 367.

[0283]Next, like the contents acquisition request T61, user side 200 is accessed to the content exhibiting distributing institution 310, and obtains contents. Namely, the content exhibiting distributing institution 310, reading the enciphered digital contents which are saved at the contents database functional block 354, if the demand of acquisition of contents is made from above-mentioned user side 200 via the communication function block 341 -- the read digital contents concerned -- user side 200 -- sending .

[0284]Then, user side 200 is accessed to accounting information control machine Seki 320 by the information claim T65 for contents appreciation, and obtains the information for contents appreciation like the information sending T66 for contents appreciation. Namely, via the communication function block 361 in accounting information control machine Seki 320, If the request for a service condition and a contents key is made as information for contents appreciation from above-mentioned user side 200, a contents key and a service condition will be published from a

contents key and the service-condition issuing function block 364, and these will be sent to user side 200 via the communication function block 361.

[0285]By the above, the flow in the case of circulation of the information for contents and contents appreciation is completed. The explanation about other composition currently mentioned to this drawing 33 is mentioned later.

[0286]Next, the principal part of the flow of balancing account, i.e., balancing account of a contents usage fee, when contents are actually appreciated is explained using drawing 34.

[0287]First, after appreciation of contents is performed in user side 200, from concerned user side 200, point usage information, i.e., use record of contents, is sent to accounting information control machine Seki 320 like the statement-of-accounts sending T71 as mentioned above. Thus, if sending of the above-mentioned contents use record is received from above-mentioned user side 200 via the communication function block 361, the contents use record concerned will be received with the balancing account procedure reception functional block 365 of accounting information control machine Seki 320, and the balancing account written confirmation corresponding to this will be published. Similarly the balancing account written confirmation concerned is sent to user side 200 via the communication function block 361 like the balancing account written confirmation sending T73. Thereby, user side 200 can know that balancing account was performed.

[0288]Next, the balancing account procedure reception functional block 365 of accounting information control machine Seki 320 makes royalty issuing information publish from the royalty issuing function block 362. This royalty issuing information is sent to the system management organization 330 via the communication function block 361 as user settlement of accounts and the contents use record sending T74 with the contents use record sent from above-mentioned user side 200.

[0289]The system management organization 330 summarizes the information sent from accounting information control machine Seki 320 currently distributed in various places with collection of money and the distribution frame block 405, totals the amount of collection of money, a collection-of-money place, and the distribution destination of money, and settles them through a actual financial institution.

[0290]By the above, the flow of balancing account of a contents usage fee is completed. The explanation about other composition currently mentioned to this drawing 34 is mentioned later.

[0291]In explanation to drawing 34, from above-mentioned drawing 30, the data transmission and reception between the content exhibiting distributing institution 310, accounting information control machine Seki 320, the system management organization 330, and user side 200, In the data transmission and reception between the content exhibiting distributing institution 310, accounting information control machine Seki 320, and the system management organization 330, it cannot be

overemphasized that a data encryption and decryption are performed like the above-mentioned. Also in this encryption and decryption, any of a public-key crypto system and a common key encryption system may be used, as mentioned above, a public-key crypto system can be used as a cipher system of a contents key or a common key, and a common key encryption system can be used as cipher systems, such as a message and various kinds of documents. It is also possible to use the technique of the improvement in security using said random number, the encryption at the time of treating contents, and least-common-multiple-ization of a compressive batch with these encryption.

[0292]Next, the concrete composition of each organizations 310, 320, and 330 mentioned above is explained briefly.

[0293]First, the composition of the content exhibiting distributing institution 310 is explained using drawing 35.

[0294]In this drawing 35, the content exhibiting distributing institution 310 concerned, The communication function block 341 which divides roughly and takes charge of the communication function between user side 200 and the system management organization 330, It consists of the contents acquisition functional block 342 which takes charge of the acquisition function of contents, the content display functional block 343 which takes charge of the exhibition function of contents, the balancing account functional block 344 which takes charge of balancing account, and the contents database functional block 345 which saves contents.

[0295]The contents bill creation function part 351 which takes charge of creation of a bill in case the above-mentioned contents acquisition functional block 342 charges contents to the system management organization 330, The contents receipt creation function part 352 which takes charge of creation of a receipt when contents are received from the system management organization 330, It consists of the function part 353 corresponding to a contents database which takes charge of correspondence with these **** and ** contents, and the contents saved at the contents database functional block 345.

[0296]The content display function part 354 which takes charge of the function for which the above-mentioned content display functional block 343 actually exhibits contents to virtual online shop, It consists of the function part 355 corresponding to a contents database which takes charge of correspondence with the contents currently these-exhibited and the contents saved at the above-mentioned contents database functional block 345.

[0297]The above-mentioned balancing account functional block 344 consists of the receipt issuing function part 356 which takes charge of the function to publish a receipt, and the function part 357 corresponding to the financial institution which takes charge of correspondence between the financial institutions 220.

[0298]Next, the composition of accounting information control machine Seki 320 is

explained using drawing 36.

[0299]In this drawing 36, accounting information control machine Seki 320 concerned, The communication function block 361 which divides roughly and takes charge of the communication function between user side 200 and the system management organization 330, The royalty issuing function block 362 which takes charge of the function to publish a royalty, A contents key, and the contents key and service-condition receipt functional block 363 which take charge of the receipt of a service condition, A contents key, and the contents key and service-condition issuing function block 364 which take charge of issue of a service condition, It consists of the balancing account procedure reception functional block 365 which takes charge of the receptionist function of balancing account procedure, the distribution receipt functional block 366 which takes charge of the function of a receipt as distribution, and the database function block 376.

[0300]The purchase written request acknowledgement function part 371 in which the above-mentioned royalty issuing function block 362 takes charge of the acknowledgement function of a purchase written request, The point-data acknowledgement function part 372 which takes charge of the check of the data of the balance (balance of point information) of the royalty of client, i.e., user, side 200, use record (point usage information), etc., The royalty generating function part 373 which takes charge of the function to generate a royalty, and the royalty invoice creation function part 374 which takes charge of the function which draws up the invoice of a royalty, It consists of a royalty, the sending function part 375 which takes charge of the function to actually send a royalty invoice, the royalty receipt acknowledgement function part 376 which takes charge of the check of the receipt document of a royalty, and the royalty issuing information preservation function part 377 which takes charge of the function to save the information on the published royalty.

[0301]Above-mentioned contents key and service-condition receipt functional block 363 consist of a contents key, the receipt function part 378 which takes charge of the receipt of a service condition, and a contents key and the preservation function part 379 which saves a service condition.

[0302]Above-mentioned contents key and service-condition issuing function block 364, A contents key and the receiving function part 380 which takes charge of the function to receive the acquisition request of a service condition, The search service part 381 which takes charge of the function which searches and discovers a contents key and a service condition from the database function block 367, It consists of the transmitting-function part 382 which takes charge of the function to encipher and send a contents key and a service condition, and a contents key and the acknowledgement function part 383 which takes charge of the acknowledgement function of the receipt document of a service condition.

[0303]The contents use record receiving function part 384 which takes charge of the function which the above-mentioned balancing account procedure reception functional block 365 receives the contents use record (point usage information) enciphered, and is decrypted, The contents use record acknowledgement function part 385 which takes charge of the check of contents use record, The contents use record-keeping function part 386 which takes charge of the function in which the database function block 367 saves contents use record, It consists of the completion document creation function part 387 which takes charge of the function which draws up the completion document of balancing account procedure, and the conclusion function part 389 which takes charge of the function to edit contents use record collectively.

[0304]The bill acknowledgement function part 390 which takes charge of the acknowledgement function of the request-for-information document which charges the data at the time of the above-mentioned distribution receipt functional block 366 collecting money, The use record report writer feature part 391 which takes charge of the function which draws up the report of the contents use record submitted to the system management organization 330, It consists of the royalty issue report writer feature part 392 which takes charge of the function which draws up the report of the royalty issuing information submitted to the system management organization 330, and the written confirmation acknowledgement function part 393 which takes charge of the acknowledgement function of the confirmation-of-receipt document of a report.

[0305]The royalty database function part 394 which takes charge of the function in which the database function block 367 saves the data of a royalty, A contents key, and the contents key and royalty database function part 395 which take charge of the function to save the data of a service condition, It consists of the user management data base function part 397 which saves the information about the contents use recording data base function part 396 which saves contents use record, and a user.

[0306]Next, the composition of the system management organization 330 is explained using drawing 37.

[0307]In this drawing 37, the system management organization 330 concerned, The communication function block 401 which divides roughly and takes charge of the communication function between user side 200, the content exhibiting distributing institution 310, and accounting information control machine Seki 320, It consists of the user subscription support functional block 402 which performs the support in the case of user subscription, the contents distribution functional block 404 which takes charge of distribution of contents, the database function block 403, and collection of money and the collection-of-money **** distribution frame block 405 which takes charge of the function of distribution.

[0308]The above-mentioned user subscription support functional block 402, Creation of a subscription request, and the subscription request creation transmitting-function

part 411 which takes charge of transmission, The common key receiving function part 412 which takes charge of the function which receives and decrypts the enciphered common key, The subscription request acknowledgement function part 413 which takes charge of the acknowledgement function of the subscription request transmitted from user side 200, The ID generating function part 414 which takes charge of the function to generate client ID, i.e., user ID, The subscription request preservation function part 415 which takes charge of the function to save a subscription request at the database function block 403, It consists of the client function generation function part 416 which generates a client function, and the registration information preservation function part 417 which takes charge of the function to save registration information at the database function block 403.

[0309]The user management data base function part 418 to which the database function block 403 carries out preservation management of a user's information, The contents database function part 419 which saves contents, and the accounting information control machine Seki database function part 420 which carries out preservation management of the information on accounting information control machine Seki 320, It consists of the content-exhibiting-distributing-institution database function part 421 which carries out preservation management of the information of the content exhibiting distributing institution 310.

[0310]The bill acknowledgement function part 422 in which the contents distribution functional block 404 takes charge of the acknowledgement function of the bill of contents, The content retrieval function part 423 which takes charge of the function to search ready-mixed concrete TENTSU (source data), i.e., the contents before processing, from the contents database function part 419 of the database function block 403, The content ID generation function part 424 which generates content ID, and the contents key generation function part 425 which generates a contents key, The contents service-condition generation function part 426 which generates a contents service condition, The contents compression function part 427 which compresses ready-mixed concrete TENTSU, i.e., the contents before processing, The preservation function part 429 which takes charge of the function to save the contents processing function part 428 which enciphers contents, and content ID, a contents key and a service condition at the contents database function part 419 of the database function block 403, The contents sending function part 430 which takes charge of the function to send contents via the communication function block 401, and the contents receipt acknowledgement function part 431 which takes charge of the function to check the receipt of contents, Content ID, a contents key, and ID, key and service-condition sending function part 432 that take charge of the function to send a service condition via the communication function block 401, It consists of content ID, a contents key, and ID, key and service-condition receipt acknowledgement function part 433 that take charge of the function to check the

receipt of a service condition.

[0311]The request-for-information document creation function part 434 which makes out the bill of the data which use collection of money and the distribution frame block 405 for collection of money, The contents royalty receiving function part 435 which takes charge of the function to receive a contents royalty via the communication function block 401, The contents use record receiving function part 436 which takes charge of the function to receive contents use record via the communication function block 401, The confirmation-of-receipt document creation function part 437 which takes charge of the function which draws up the written confirmation of reception, It consists of the calculation and the bill creation function part 438 which makes out the bill which performs the calculation of the amount billed and the creation of a bill which are charged to a user, calculation of the dividend at the time of distributing the use gold collected by use to a right holder, and the calculation and the form-for-payment creation function part 439 which perform creation of a form for payment.

[0312]next -- being concerned -- others -- the composition of user side 200 corresponding to the system of an embodiment is explained using drawing 38. This drawing 38 expresses each function of said player 1 and the user terminal 50 collectively.

[0313]In this drawing 38, the composition of concerned user side 200, The communication function block 451 which will take charge of the communication function between the system management organization 330, the content exhibiting distributing institution 310, and accounting information control machine Seki 320 if it divides roughly, The contents acquisition functional block 452 which takes charge of acquisition of contents, The royalty purchasing function block 453 which takes charge of the purchase of royalties, such as point information, a contents key, a service condition, A contents key, and the contents key and service-condition acquisition functional block 454 which take charge of acquisition of a service condition, The balancing account procedure functional block 455 which takes charge of balancing account procedure, and the user subscription support functional block 456 which takes charge of the function which supports subscription to a system, It consists of appreciation of contents, the contents appreciation accounting function block 457 which takes charge of the function of fee collection, and the database function block 458.

[0314]The above-mentioned contents acquisition functional block 452 consists of the contents acquisition function part 461 which takes charge of the function which actually obtains contents, and the contents preservation function part 462 which takes charge of the function in which contents are made to save at a memory medium.

[0315]The purchase written request creation function part 463 in which the royalty purchasing function block 453 draws up the purchase written request of a royalty, The conclusion function part 464 which takes charge of the conclusion of the data of the

balance (point balance) of the royalty of a client (user), use record (point usage information), etc., It consists of the royalty installation function part 465 which takes charge of the function which installs each information as a royalty, and the royalty receipt document creation function part 467 which draws up a royalty receipt document.

[0316]A contents key and the service-condition acquisition functional block 454, It consists of a contents key, the acquisition written request creation function part 468 which draws up the acquisition written request of a service condition, a contents key and the receiving function part 469 which takes charge of reception of a service condition, and a contents key and the receipt document creation function part 470 which draws up the receipt document of a service condition.

[0317]The balancing account procedure functional block 455 consists of the conclusion function part 471 which performs the conclusion of contents use record (point usage information), and the completion document receiving function part 472 which takes charge of reception of the completion document of balancing account procedure.

[0318]The above-mentioned user subscription support functional block 456, It consists of the subscription request creation function part 473 which takes charge of creation of a subscription request, the client function installation function part 474 which takes charge of installation of a client function, i.e., initialization of a user's player 1, and the registration information creation function part 475 which takes charge of the function which creates registration information.

[0319]The content retrieval function part 476 which takes charge of search of the contents by which the contents appreciation accounting function block 457 was saved at the memory medium, The royalty acknowledgement function part 477 which takes charge of the check of a royalty, and the simple contents appreciation function part 478 which reproduces contents in [when choosing contents, for example] simple, The accounting function part 479 which manages accounting information (point information), and the contents function decoding part 480 which decrypts the contents enciphered, It consists of the contents extension function part 481 which elongates the contents compressed, and the contents viewer function part 482 for enabling recognition of the contents of the contents saved at the memory medium, for example.

[0320]The royalty database function part 483 where the database function block 458 saves the data of a royalty, It consists of a contents key, the contents key and service-condition database function part 484 which save a service condition, the contents use recording data base function part 485 which saves contents use record, and the user information data base function part 486 which saves User Information.

[0321]Next, the player 1 of each embodiment which was mentioned above, and the concrete using form of the user terminal 50 are explained using drawing 39 and

drawing 40.

[0322]As shown in drawing 39, the player 1 is arranged after said analog output terminal 2, the interface terminal 3 for PC, and the I/O terminal 4 for memory media have projected out of the case of the player 1, and the memory medium 61 is connected to the above-mentioned I/O terminal 4 for memory media. For example in the case 60, these players 1 and the memory medium 61 are formed so that storage is possible, and they are made as [arrange / for example at the end side of this case 60 / the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC].

[0323]The case 60 where this player 1 and memory medium 61 were stored, From the side by which the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC are arranged, it is formed in the input/output port 53 of the personal computer 50 as the above-mentioned user terminal 50 so that insertion connecting may be possible.

[0324]Although the personal computer 50 concerned has the general composition which equipped the computer body with the display device 52, the keyboard 54, and the mouse 55, In the above-mentioned input/output port 53, the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC, and the corresponding interface are formed. Therefore, only by inserting in the input/output port 53 of the above-mentioned personal computer 50 the case 60 where the above-mentioned player 1 and the memory medium 61 were stored, The analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC come to be connected with the above-mentioned personal computer 50.

[0325]Although he is trying to form an interface [in the input/output port 53 of the personal computer 50 / terminal / 3 / for PC / the analog output terminal 2 of the above-mentioned player 1, and / interface] in the example of above-mentioned drawing 39, For example, as shown in drawing 40, it is also possible to arrange the adapter 62 which can respond to the interface of the general-purpose input/output port of the personal computer 50 between the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC.

[0326]In the system of an embodiment of the invention since it has stated above, Since digital contents are enciphered with the contents key which is a common key of a system, If it is the user (player 1) who registered with the system of this embodiment, if only it can copy these enciphered contents freely and a contents key comes to hand, appreciation of these contents is also possible. Therefore, installation to this contents memory medium (enciphered contents) can also be performed easily. On the other hand, since the enciphered digital contents cannot be decoded, the right of the copyright of contents or the right holder of the contents concerned is protected by the terminal unit which is not based on this embodiment system.

[0327]an embodiment of the invention, while according to the system filling up point

information with a prepaid system (charge advance payment method) and reducing point information at the time of contents appreciation, Since he is trying to collect the usage information of the point, recovery of an appreciation price is possible for right holders (owner of a copyright etc.), a contents selling store, etc. with the right about a used point.

[0328]Since encryption is given in the case of an exchange of the data of point information or point usage information as mentioned above, security nature is improving. For example, since it shall trade after checking that use the random number (security ID) which interlocked by the system and player side, and both are in agreement, as mentioned above even if the completely same thing as the last data is forged and it tries to steal the point information for fee collection, it is safe.

[0329]1 chip making of the main components of a player is carried out, and it is difficult to take out key information and the decrypted digital contents outside. This player 1 equips player 1 the very thing with the tamper resistance function, in order to prevent the data usurpation by destruction of the player 1 concerned.

[0330]As mentioned above, according to the embodiment of the invention, the digital contents distributing system with high security top intensity is built.

[0331]As above-mentioned digital contents, various kinds of things other than digital audio information, such as a digital video data, can be mentioned. When dynamic-image-data (audio information is also included) use is carried out as the above-mentioned digital video data, as the technique of said compression, compression methods, such as MPEG (Moving Picture Image CodingExperts Group), can be used, for example. The above-mentioned MPEG, In WG(Working Group) 11 of SC(Sub Committee) 29 of JTC(Joint Technical Committee)1 of ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). It is a common name of the packed video coding mode, and there are MPEG1, MPEG 2, MPEG4, etc.

[0332]As the technique of the above-mentioned encryption, as mentioned above, the enciphering method currently called what is called DES (Data Encryption Standard) can be used. DES is the standard cipher system (cryptographic algorithm) which NIST (National Institute of Standards and Technology) in the U.S. announced in 1976. Data conversion is performed for every 64-bit data block, and, specifically, the conversion using a function is repeated 16 times. The above-mentioned digital contents, point information, etc. are enciphered with what is called a common key system using the DES concerned. It is a method which becomes the same [the key (decode key data) for decrypting with the key data (encryption key data) for enciphering] as that of the above-mentioned common key system.

[0333]What is called an EEPROM (electrically eliminable ROM) can be used for the common key storage memory 22 of the player 1 of said drawing 1, the key storage memory 21 for communication, the point usage information storing memory 29, and

point information storing memory 28 grade, for example.

[0334]As a memory medium, the memory medium of recording media, such as a hard disk, a floppy disk, a magneto-optical disc, and a phase-change optical disk, or semiconductor memory (IC card etc.) can be used for others, for example.

[0335]In addition, although selection, a check, etc. were performed in the above-mentioned embodiment using the keyboard 54 of the user terminal 50, and the mouse 55 and the display device 52 on the occasions, such as content confirmation etc. of the contents exhibited by selection and the virtual online shop 230 of contents, It is also possible to simplify a function to these keyboards, or a mouse and a display device, and to give the player 1. namely, . Like drawing 2, it is also possible to form the input key part 6 and the indicator 7 in the player 1.

[0336]

[Effect of the Invention]It is possible to be able to do carrying simply in the above explanation, according to this invention so that clearly, and to enjoy digital contents anywhere always, It is possible also in it being equal to employment enough as the copy of digital contents, or defense to unjust use, and building an economical system.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a system configuration figure showing the entire configuration of the digital contents distribution system of an embodiment of the invention.

[Drawing 2]It is a block circuit diagram showing the concrete composition of the player corresponding to the system of an embodiment of the invention.

[Drawing 3]It is a block circuit diagram showing the concrete composition of the control center corresponding to the system of an embodiment of the invention.

[Drawing 4]It is a figure used for explanation of the procedure at the time of the purchase of a player in the system of this embodiment.

[Drawing 5]It is a figure used for explanation of the procedure to installation of the digital contents from search of digital contents to the memory medium for players in the system of this embodiment.

[Drawing 6]It is a figure used for explanation of the procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for fee collection in the system of an embodiment.

[Drawing 7]It is a figure used for explanation of the procedure of distribution of a fee collection price in the system of an embodiment.

[Drawing 8]It is a flow chart which shows the flow of the processing in the player at the time of point purchase in the system of an embodiment.

[Drawing 9]It is a flow chart which shows the flow of the processing in the user terminal at the time of point purchase in the system of an embodiment.
[Drawing 10]It is a flow chart which shows the flow of the processing in the control center at the time of point purchase in the system of an embodiment.
[Drawing 11]It is a figure showing the sequence of the information transmission and reception at the time of point purchase in the system of an embodiment.
[Drawing 12]It is a flow chart which shows the flow of the processing in the player at the time of acquisition of digital contents in the system of an embodiment.
[Drawing 13]It is a flow chart which shows the flow of the processing in the user terminal at the time of acquisition of digital contents in the system of an embodiment.
[Drawing 14]It is a flow chart which shows the flow of the processing in the control center at the time of acquisition of digital contents in the system of an embodiment.
[Drawing 15]It is a figure showing the sequence of the information transmission and reception at the time of acquisition of digital contents in the system of an embodiment.
[Drawing 16]It is a flow chart which shows the flow of the processing in the player at the time of acquisition of a contents key and a service condition in the system of an embodiment.
[Drawing 17]It is a flow chart which shows the flow of the processing in a contents key and the user terminal at the time of acquisition of a service condition in the system of an embodiment.
[Drawing 18]It is a flow chart which shows the flow of the processing in the control center at the time of acquisition of a contents key and a service condition in the system of an embodiment.
[Drawing 19]It is a figure showing the sequence of the information transmission and reception at the time of acquisition of a contents key and a service condition in the system of an embodiment.
[Drawing 20]It is a flow chart which shows the flow of the processing at the time of actually appreciating digital contents using a player and a user terminal in the system of an embodiment.
[Drawing 21]It is a flow chart which shows the flow of the processing in the player at the time of point usage information return in the system of an embodiment.
[Drawing 22]It is a flow chart which shows the flow of the processing in the user terminal at the time of point usage information return in the system of an embodiment.
[Drawing 23]It is a flow chart which shows the flow of the processing in the control center at the time of point usage information return in the system of an embodiment.
[Drawing 24]It is a figure showing the sequence of the information transmission and reception at the time of point usage information return in the system of an embodiment.
[Drawing 25]It is a flow chart which shows the flow of the processing at the time of performing decryption and extension in the least common multiple of the batch of

encryption and compression.

[Drawing 26]It is a block circuit diagram showing the composition which performs encryption, decryption for every unit of the least common multiple of a compressive batch, and elongation processing.

[Drawing 27]It is a block circuit diagram showing the concrete composition which generates the random number as security ID.

[Drawing 28]When enciphering a common key with a public-key crypto system and transmitting, it is a figure for explaining signs that a random number is inserted.

[Drawing 29]It is a figure for explaining signs that a random number is taken out from a receiving sentence and the check of justification is made.

[Drawing 30]It is a figure used for explanation of each organization when the function by the side of a system is divided.

[Drawing 31]In the embodiment which divided the function by the side of a system, it is a figure for explaining the principal part of the flow of the time of subscription to a user's system.

[Drawing 32]In the embodiment which divided the function by the side of a system, it is a figure for explaining the principal part of the information flow at the time of acquisition of the key the purchase of point information, and for decoding of the enciphered digital contents, etc.

[Drawing 33]In the embodiment which divided the function by the side of a system, it is a figure for explaining the principal part of the flow in the case of circulation of the information for contents and contents appreciation.

[Drawing 34]In the embodiment which divided the function by the side of a system, it is a figure for explaining the principal part of the flow of balancing account when contents are actually appreciated.

[Drawing 35]In the embodiment which divided the function by the side of a system, it is a block diagram showing the composition of content exhibiting distributing institution.

[Drawing 36]In the embodiment which divided the function by the side of a system, it is a block diagram showing the composition of accounting information control machine Seki.

[Drawing 37]In the embodiment which divided the function by the side of a system, it is a block diagram showing the composition of a system management organization.

[Drawing 38]In the embodiment which divided the function by the side of a system, it is a block diagram showing users' composition.

[Drawing 39]It is a figure used for explanation of an example of the concrete using form of a player and a user terminal.

[Drawing 40]It is a figure used for explanation of other examples of the concrete using form of a player and a user terminal.

[Drawing 41]It is an example of composition of performing anti-copying or fee

collection using the conventional compression/extension art, and is a block circuit diagram showing the composition which enciphers after compression.

[Drawing 42]It is a flow chart which shows decryption and the flow at the time of carrying out elongation processing for the data in which encryption was performed after compression by a receiver.

[Drawing 43]It is an example of composition of performing anti-copying or fee collection using the conventional compression/extension art, and is a block circuit diagram showing the composition which compresses after encryption.

[Description of Notations]

1 A player, 2 analog output terminals, the interface terminal for 3 PC, 4 The I/O terminal for memory media, and 16 A controller and 19 Security ID generating circuit, 20 An open code decoder circuit and 21 The key storage memory for communication, and 22 Common key storage memory, 23 A user ID storing memory and 24 A common code decoder circuit and 25 buffer memories, 26 An expansion circuit, 27 D/A conversion circuits, 50 user terminals, and a 100 contents-managing functional block, A 110 user-management functional block and 120 [A financial institution and 230 / Virtual online shop and 240 / Content provider] A usage information controlling-function block and 130 A controlling-function block and 200 The user side, 210 system management companies, 211 control centers, and 220

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－271011

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０３Ｍ	7/30		Ｈ０３Ｍ	7/30	Ｚ
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ａ
		６６０			６６０Ｆ

審査請求　未請求　請求項の数５　ＯＬ　（全 39 頁）

(21)出願番号　特願平9－74184

(22)出願日　平成９年(1997)３月26日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　真有　浩一
東京都品川区北品川６丁目７番35号　ソニー株式会社内

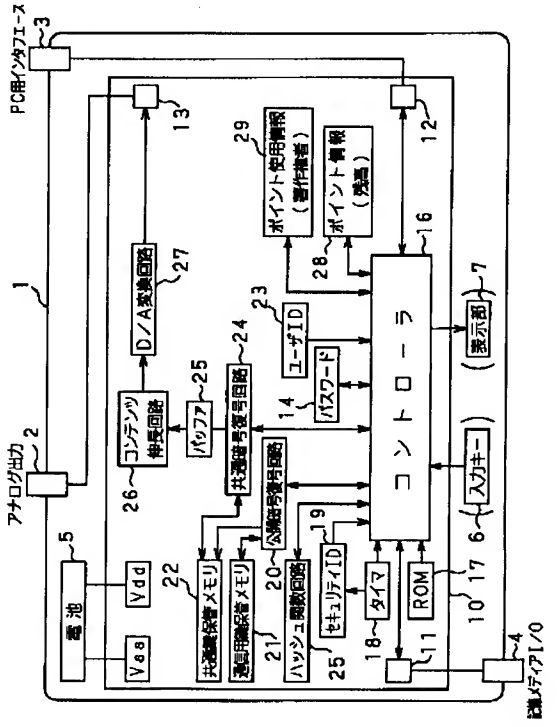
(74)代理人　弁理士　小池　晃　（外２名）

(54)【発明の名称】　データ処理方法及び装置

(57)【要約】

【課題】　ネットワークを使って配信するディジタルデータの安全性を向上させる。

【解決手段】　暗号化及び圧縮されたディジタルデータを復号化アルゴリズムの処理ビット数毎に復号化する共通鍵暗号復号回路２４と、この復号化されたデータを上記復号化アルゴリズムの処理ビット数と伸長アルゴリズムの処理ビット数の最小公倍数のビット単位で一時保存するバッファメモリ２５と、このバッファメモリ２５に保存したデータを伸長アルゴリズムの処理ビット数毎に読み出して伸長する伸長回路２６とを有する。



【特許請求の範囲】
【請求項１】　暗号化及び圧縮されたディジタルデータを、上記暗号化に対応する復号化アルゴリズムの処理ビット数と、上記圧縮に対応する伸長アルゴリズムの処理ビット数との最小公倍数のビット単位にて一括して復号化及び伸長することを特徴とするデータ処理方法。
【請求項２】　上記暗号化及び圧縮されたディジタルデータを上記復号化アルゴリズムの処理ビット数毎に復号化し、
当該復号化されたデータを上記最小公倍数のビット単位で一時保存し、
上記保存したデータを上記伸長アルゴリズムの処理ビット数毎に読み出して伸長することを特徴とする請求項１記載のデータ処理方法。
【請求項３】　暗号化及び圧縮されたディジタルデータを、上記暗号化に対応する復号化アルゴリズムの処理ビット数と、上記圧縮に対応する伸長アルゴリズムの処理ビット数との最小公倍数のビット単位にて一括して復号化及び伸長する復号伸長手段を有することを特徴とするデータ処理装置。
【請求項４】　上記復号伸長手段は、上記暗号化及び圧縮されたディジタルデータを上記復号化アルゴリズムの処理ビット数毎に復号化する復号化手段と、当該復号化手段にて復号化されたデータを上記最小公倍数のビット単位に一時保存する保存手段と、上記保存手段に保存したデータを上記伸長アルゴリズムの処理ビット数毎に読み出して伸長する伸長手段とを有することを特徴とする請求項２記載のデータ処理装置。
【請求項５】　上記復号伸長手段は、集積回路内に配されてなることを特徴とする請求項４記載のデータ処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えば暗号化及び圧縮されたディジタルデータを復号伸長する際のデータ処理方法及び装置に関する。
【０００２】
【従来の技術】コンピュータプログラムやオーディオデータ，ビデオデータ等のディジタルコンテンツの流通を簡便化し、潜在需要を掘り下げ、市場拡大に有利な手法としては、例えば特公平６－１９７０７号公報に記載されるソフトウェア管理方式、特公平６－２８０３０号公報に記載されるソフトウェア利用管理方式、特公平６－９５３０２号公報に記載されるソフトウェア管理方式のような手法が存在する。上記特公平６－１９７０７号公報に記載されたソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、ソフトウェアの利用状況をソフトウェア権利者別などによって把握できるようにしたものである。また、特公平６－２８０３０号公報に記載されるソフトウェア利用管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラムを買い取り（買い取った後は無料で使用できる）価格を付し、コンピュータシステム内には購入可能な金額を示すデータを設けておき、有償プログラム購入の際は、同システムにある利用可能なソフトウェアの名称としてテーブルに登録すると共に、当該購入可能金額を示すデータをソフトウェア価格分だけ減じ、また登録済みソフトウェアを該テーブルから抹消する際には状況に応じて該購入可能な金額を示すデータを増加更新するようにしたものである。また、上記特公平６－９５３０２号公報に記載されるソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラムにつき実際の利用量（利用回数または利用時間など）に応じて利用料金を徴収するために、利用されたプログラムの識別と「利用者識別符号と料金とを記録」しておき、該記録を回収することでプログラム権利者が自分の所有するプログラムの利用料金を把握でき、プログラムの利用量に応じたプログラム利用料金を回収する場合のシステムで有効なものである。
【０００３】
【発明が解決しようとする課題】ところで、上述したように、ネットワークを使ってディジタルコンテンツを配信する際には、そのデータ量を抑えるために圧縮／伸長技術を使用し、コピー防止或いは課金のために暗号化／圧縮技術が使われる。
【０００４】すなわち、図４１に示すように、ディジタルコンテンツの配信時には、配信側の圧縮処理部７００にてディジタルコンテンツを圧縮し、さらに暗号化処理部７０１にて暗号化処理することが行われる。上述の例のように配信側にて生成されたディジタルコンテンツ（圧縮／暗号化データ）をネットワークを使って配信したとすると、当該圧縮／暗号化されたディジタルコンテンツを受信した受信側では、復号化処理部７０２にて上記圧縮及び暗号化されているディジタルコンテンツを復号化し、さらに伸長処理部７０３にて伸長してディジタルコンテンツを復元することが行われる。なお、以下に言う復号化とは、暗号化を解くことである。
【０００５】この図４１のようなシステム構成において、受信側での復号化及び伸長処理の流れは、より具体的には図４２のフローチャートにて表すことができる。
【０００６】この図４２において、図４１の受信側の復号化処理部７０２には、ステップＳＴ５０１に示すように、配信側からネットワークを介して上記圧縮及び暗号化されたディジタルコンテンツが入力される。この圧縮及び暗号化されているディジタルコンテンツのデータは、当該復号化処理部７０２にて、ステップＳＴ５０２のように、復号化処理のアルゴリズムに従った処理単位Ｘビット毎に分割され、さらにステップＳＴ５０３のよ

うに当該Ｘビット毎の処理単位毎に復号鍵を元にして順次復号化される。その後、当該復号化処理部７０２では、ディジタルコンテンツの全データについて上記復号化処理が完了したか否かを判断し、完了していないときにはステップＳＴ５０２に戻って上述の処理を繰り返し、完了したときには、ステップＳＴ５０５のように、上記復号化処理されたディジタルコンテンツの全データを、次段の伸長処理部７０３に送る。

【０００７】この伸長処理部７０３では、上記伸長復号化により得られた全データ、すなわち圧縮されているディジタルコンテンツを、ステップＳＴ５０６に示すように、圧縮伸長処理のアルゴリズムに従った処理単位Ｙビット毎に分割する。同時に、この伸長処理部７０３では、ステップＳＴ５０７のように当該Ｙビット毎の処理単位毎に、上記圧縮ディジタルコンテンツを順次伸長処理する。その後、当該伸長処理部７０３では、ディジタルコンテンツの全データについて上記伸長処理が完了したか否かを判断し、完了していないときにはステップＳＴ５０５に戻って上述の処理を繰り返し、完了したときには、ステップＳＴ５０８のように、上記伸長処理されたディジタルコンテンツの全データを後段に出力する。

【０００８】なお、上記暗号化と圧縮、復号化と伸長の処理の順番は入れ替わる場合もある。すなわち、図４３に示すように、配信側の暗号化処理７０４にてディジタルコンテンツを暗号化し、さらに圧縮処理部７０５にて圧縮処理することが行われた場合、当該暗号／圧縮化されたディジタルコンテンツをネットワークを介して受信した受信側では、伸長処理部７０６にて上記暗号化及び圧縮されているディジタルコンテンツを伸長し、さらに復号化処理部７０７にて伸長してディジタルコンテンツを復元することが行われる。

【０００９】上述したように、従来の技術によれば、受信側において、復号化処理と伸長処理の何れの場合も、それぞれディジタルコンテンツの全データの処理が終了するまで続けられるようになっている。

【００１０】ここで、上記図４１の受信側の復号化処理部７０２の全出力データ、或いは図４３の受信側の伸長処理部７０６の全出力データは、それぞれデータ量が非常に大きいものである。このため、上記図４１の復号化処理部７０２の全出力データ、或いは図４３の伸長処理部７０６の全出力データは、それぞれ次段の構成に送られる前に、ビット単価の安価な外部メモリに一旦保存されることが多い。

【００１１】この外部メモリに保存されたデータは、比較的容易に取り出すことができる。

【００１２】したがって、例えば悪意を持った者が、上記外部メモリからデータを盗むことは非常に容易である。

【００１３】特に、図４１の例のように外部メモリに復号化後のデータが保存されることになる場合には、当該復号化されたデータからは容易に元のディジタルコンテンツを復元することが容易であるため、当該保存されたデータが盗まれることは問題である。

【００１４】すなわち、圧縮に対する伸長方式のアルゴリズムは一般に公開されている場合が多く、また伸長方式のアルゴリズムには一般的な暗号鍵のようにそれぞれ隠しておけば復号化の処理ができないようなものも存在していない。しかも、上記復号化された後の圧縮ディジタルコンテンツは、上記送信側から配信された暗号化と圧縮がなされたディジタルコンテンツと比較して、データ量的に変わらず、したがって、上記復号化された圧縮ディジタルコンテンツを悪意を持ってさらに別の者に配信することも容易である。

【００１５】さらに、上記ディジタルコンテンツに著作権等が存在する場合、上記受信側は、上記ディジタルコンテンツを上記復号化及び伸長する際に、上記著作権者等の意思に従って課金されることになるが、上述のように復号化された後のディジタルコンテンツが盗難されるようなことが起これば、著作権者等の意思の届かないところでさらに別の者に配信されたり、伸長されたりする危険性が大きい。

【００１６】そこで、本発明はこのような状況に鑑みてなされたものであり、ネットワークを使って配信するディジタルデータの安全性を向上させることが可能なデータ送受信方法及び装置を提供することを目的とする。

【００１７】

【課題を解決するための手段】本発明によれば、暗号化及び圧縮されたディジタルデータを、復号化アルゴリズムの処理ビット数と伸長アルゴリズムの処理ビット数との最小公倍数のビット単位にて一括して復号化及び伸長することにより、上述した課題を解決する。

【００１８】

【発明の実施の形態】以下、本発明の好ましい実施の形態について、図面を参照しながら説明する。

【００１９】先ず、本発明のデータ処理方法及び装置の具体的内容及び構成の説明を行う前に、これらの理解を容易にするために、本発明が適用されるシステム全体の概略構成及びシステムの運用方法について図１から図７までの各図を用いて簡単に説明する。

【００２０】図１にはシステム全体の概略的な構成を示す。

【００２１】この図１において、ユーザ側２００は、本発明のディジタルコンテンツ再生装置（以下、プレーヤ１と呼ぶことにする）及びいわゆるパーソナルコンピュータ（以下、ユーザ端末５０と呼ぶことにする）を保有しているものとする。

【００２２】ユーザ端末５０は、通常のパーソナルコンピュータであるが、本発明に使用する後述する各種ソフトウェアをアプリケーションソフトとして格納してなると共に、表示手段であるディスプレイ装置と放音手段で

あるスピーカ、及び情報入力手段であるキーボードやマウス等が接続されてなるものである。当該ユーザ端末５０は例えばネットワークを介してシステム管理会社２１０と接続可能であり、また、プレーヤ１との間のインターフェイス手段を有し、データ送受が可能である。

【００２３】プレーヤ１は例えば図２に示すような構成を有するものである。

【００２４】この図２の構成の詳細な説明については後述するが、当該プレーヤ１は、ディジタルコンテンツの処理経路の主要構成要素として、暗号化されているディジタルコンテンツをコンテンツ鍵を用いて復号化する共通鍵暗号復号回路２４と、圧縮されているディジタルコンテンツを伸長する伸長手段である伸長回路２６と、ディジタルデータをアナログ信号に変換するＤ／Ａ変換回路２７とを少なくとも有する。なお、以下に言う復号化とは、暗号化を解くことである。

【００２５】また、このプレーヤ１は、使用するディジタルコンテンツの権利情報及び使用状況を示す情報（以下、これら情報をポイント使用情報と呼ぶ）や、ディジタルコンテンツを使用する際に必要となる保有金額データ、すなわちディジタルコンテンツを使用する毎に減額される課金データ（以下、ポイント情報と呼ぶ）等を扱う主要構成要素として、上記ポイント使用情報を格納するポイント使用情報格納メモリ２９と、上記ポイント情報を格納するポイント情報格納メモリ２８とを少なくとも備えている。

【００２６】さらに、このプレーヤ１は、後述するような暗号化及び復号化に使用する各種鍵を格納するための構成として共通鍵保管メモリ２２及び通信用鍵保管メモリ２１と、これらに格納された鍵を用いて暗号化や復号化を行うための構成として共通暗号復号回路２４及び公開暗号復号回路２０を有している。また、このプレーヤ１は、上記暗号化及び復号化に関連する構成として、システム管理会社２１０のホストコンピュータと連動した乱数を発生してセキュリティＩＤを生成するセキュリティＩＤ発生回路１９及びタイマ１８や、後述するいわゆるハッシュ値を発生するハッシュ関数回路２５等をも有している。

【００２７】その他、当該プレーヤ１は、ディジタルコンテンツやその他各種のデータ及び各構成要素の制御をＲＯＭ１７に格納されたプログラムに基づいて行う制御手段であるコントローラ１６と、携帯時の動作電源としての電池５を備えている。

【００２８】ここで、図２のプレーヤ１の各主要構成要素は、セキュリティ上、ＩＣ（集積回路）或いはＬＳＩ（大規模集積回路）の１チップで構成されることが望ましい。この図２では、各主要構成要素が集積回路１０内に１チップ化されている。当該プレーヤ１には、外部とのインターフェイス用として３つの端子（アナログ出力端子２と、ＰＣ用インターフェイス端子３と、記録メディア用Ｉ／Ｏ端子４）を備え、これら各端子が集積回路１０のそれぞれ対応する端子１３、１２、１１に接続されている。なお、これら各端子は統合することも、また新たに別の端子を設けることも可能であり、特にこだわるものではない。

【００２９】システム管理会社２１０は、システム全体を管理する管理センタ２１１と、上記プレーヤ１を販売する販売店２１２とからなり、仮想店舗２３０を介してユーザ側２００のユーザ端末５０との間で、後述するようなディジタルコンテンツの供給に関する情報の送受、コンテンツプロバイダ２４０が保有するコンテンツを圧縮及び暗号化するディジタルコンテンツの加工、上記加工したディジタルコンテンツの供給、金融機関２２０との間の情報送受等を行う。なお、システム管理会社２１０と金融機関２２０との間では、ユーザ側２００の口座番号やクレジット番号，名前や連絡先等の確認や、ユーザ側２００との間で取引可能かどうかの情報等のやり取りなどが行われる。金融機関２２０とユーザ側２００との間では、実際の代金振込等の処理が行われる。また、販売店２１２は、必ずしもシステム管理会社２１０内に含まれる必要はなく、販売代理店であってもよい。

【００３０】上記システム管理会社２１０の管理センタ２１１は、例えば図３に示すような構成を有するものである。この図３の構成の詳細な説明については後述するが、主要構成要素として、ディジタルコンテンツを管理し、その展示、暗号化及び圧縮等の加工処理、ディジタルコンテンツの暗号化及び復号化に使用する鍵情報であるコンテンツ鍵やＩＤの発生等の各機能を有するコンテンツ管理機能ブロック１００と、ユーザ情報を管理し、通信文（メッセージやポイント情報等）の暗号化及び復号化、確認メッセージの発生、セキュリティＩＤの発生、金融機関２３０との間での決済申請、ポイントの発生等の各機能の他、ユーザ加入処理等を行うユーザ加入処理機能部１１８をも備えたユーザ管理機能ブロック１１０と、ポイント使用情報等を管理する使用情報管理機能ブロック１２０と、システム全体を管理し、通信機能を有する管理機能ブロック１３０とを、少なくとも有してなる。

【００３１】上述した図１のように構成されるシステムの実際の運用方法の一例を、図４～図７を用いて説明する。なお、以下の運用方法は、ユーザ側２００やシステム管理会社２１０，金融機関２２０，コンテンツプロバイダ２４０等が実際に行う手順である。

【００３２】このシステムの運用方法の説明では、プレーヤ１の購入の手順、ディジタルコンテンツの検索からプレーヤ１用の記憶メディアに対するディジタルコンテンツのインストールまでの手順、当該ディジタルコンテンツを使用可能にするための課金用のポイント情報の購入と当該ディジタルコンテンツを使用した場合の精算の手順、ディジタルコンテンツの鑑賞に伴ってユーザから

徴収した課金代金の分配の手順について順番に説明する。

【００３３】先ず、プレーヤ１の購入時の手順としては、図４の（１）及び（５）に示すように、ユーザ側２００が実際に店頭或いは通信販売等により、上記販売店２１２から上記プレーヤ１を購入する。

【００３４】このとき、上記販売店２１２は、図４の（２）に示すように、上記プレーヤ１の販売時に上記ユーザ側２００から提供された個人情報（名前や連絡先等）及び決済情報（銀行口座、クレジット番号等）と、上記販売したプレーヤ１固有の番号（プレーヤ固有鍵等を含む）とをシステム管理会社２１０の管理センタ２１１に登録する。

【００３５】管理センタ２１１は、図４の（３）に示すように、金融機関２２０に対して、上記ユーザ側２００から提供された口座番号やクレジット番号等の確認を行い、図４の（４）に示すように金融機関２２０から取引可能である旨の情報を得る。

【００３６】次に、ディジタルコンテンツの検索からプレーヤ１用の記憶メディアへのディジタルコンテンツのインストールまでの手順として、上記プレーヤ１を購入したユーザ側２００は、当該プレーヤ１とのインターフェイス手段を備えたユーザ端末５０を使って、図５の（１）に示すように、希望のディジタルコンテンツの検索，選択，編集，注文等を行う。このときの検索から注文までの処理は、ユーザ端末５０がアプリケーションソフトとして格納している検索ソフトを用い、例えばネットワークを介して接続された仮想店舗２３０に対して行う。

【００３７】仮想店舗２３０は、例えば管理センタ２１１がネットワーク上の仮想的に設けている店舗であり、この仮想店舗２３０には、例えば複数のコンテンツの内容を示す情報が展示されている。ユーザ側２００は、仮想店舗２３０にて提供されているこれらの情報に基づいて、所望のコンテンツの注文を行うことになる。なお、仮想店舗２３０に展示されるコンテンツの内容を示す情報としては、例えばコンテンツが映画等のビデオデータである場合には当該映画等のタイトルや広告、当該映画中の１シーン等の映像などが考えられ、また、コンテンツがオーディオデータである場合は曲名やアーティスト名、当該曲の最初の数フレーズ（いわゆるイントロ）等が考えられる。したがって、ユーザ側２００のユーザ端末５０にて上記仮想店舗２３０をアクセスした場合には、当該ユーザ端末５０上に上記仮想店舗２３０の複数のコンテンツの内容が仮想的に展示され、これら展示物の中から所望のものを選択することでコンテンツの注文が行われることになる。

【００３８】上記ユーザ側２００のユーザ端末５０からディジタルコンテンツの注文等があったとき、上記仮想店舗２３０は、図５の（２）に示すように管理センタ２１１に対してディジタルコンテンツの供給依頼を行う。

【００３９】当該ディジタルコンテンツの供給依頼を受け取った管理センタ２１１は、コンテンツプロバイダ２４０に対して上記供給依頼のあったディジタルコンテンツの配給依頼を行う。これにより、当該コンテンツプロバイダ２４０は、図５の（４）に示すように上記配給依頼のあったディジタルコンテンツを管理センタ２１１に配給する。

【００４０】管理センタ２１１は、上記コンテンツプロバイダ２４０から配給されたディジタルコンテンツに対して暗号化及び所定の圧縮方式を用いた圧縮を施すと共に、この圧縮及び暗号化されたディジタルコンテンツに対して、当該コンテンツのＩＤ（コンテンツＩＤ）とこのコンテンツの著作権者等の権利者情報と当該コンテンツを使用したときの課金額とコンテンツをユーザ側２００に供給する仮想店舗名等とを付加する。なお、コンテンツに対する課金額は、コンテンツプロバイダ２４０にて事前に決定される。

【００４１】上記管理センタ２１１にて加工されたコンテンツは、図５の（５）に示すように、仮想店舗２３０に送られ、さらにこの仮想店舗２３０を介して、図５の（６）のようにユーザ側２００のユーザ端末５０に供給される。これにより、プレーヤ１には、上記ユーザ端末５０からコンテンツが供給され、このコンテンツが当該プレーヤ１に格納されることになる。

【００４２】なお、この図５に（２）～（５）までの流れについては、事前に行っておくことも可能である。すなわち、仮想店舗２３０には、上記複数のコンテンツの内容を示す情報を展示するだけでなく、これら展示に対応した上記加工されたディジタルコンテンツを予め用意しておくようにしても良い。

【００４３】次に、上述のようにしてプレーヤ１にインストールされたディジタルコンテンツを使用可能にするための課金用のポイント情報の購入と当該ディジタルコンテンツを使用した場合の精算の手順では、先ず、ユーザ端末５０によってプレーヤ１に格納されているポイント情報の不足が確認されて、当該ユーザ端末５０からポイント情報の補充要求がなされる。

【００４４】このとき、図６の（１）のように、当該ユーザ端末５０からは、プレーヤ１にて暗号化されたポイント情報の補充依頼が、管理センタ２１１に対し転送される。また同時に、既に使用したディジタルコンテンツに対応する著作権者等の権利者の情報すなわちポイント使用情報がプレーヤ１から読み出されて暗号化され、ユーザ端末５０を介して管理センタ２１１に送られる。このように、ポイント情報の補充依頼と同時にポイント使用情報の転送が行われるようにしたのは、当該ポイント使用情報の管理センタ２１１への送信のみのために、ユーザ側２００が管理センタ２１１にアクセスする手間を省くためである。勿論、このポイント使用情報の転送

は、必ずしもポイント情報の購入と同時に行う必要はなく、独立に行っても良い。

【００４５】上記暗号化されたポイント情報の補充依頼及びポイント使用情報を受け取った管理センタ２１１は、当該暗号を解読することでユーザ側２００が要求しているポイント情報の補充量とポイント使用情報の内容を認識する。さらに、当該管理センタ２１１は、金融機関２２０に対して図６の（２）のように当該ポイント補充分の決済が可能かどうかの確認を行う。金融機関２２０にて、ユーザ側２００の口座を調べることによって、決済可能であることが確認されると、当該金融機関２２０から図６の（３）のように決済ＯＫの指示が管理センタ２１１に送られることになる。

【００４６】また、このときの管理センタ２１１は、図６の（４）に示すように、コンテンツプロバイダ２４０に対して著作権者等の権利者に支払われることになるポイント使用数、すなわち金額を連絡する。

【００４７】その後、管理センタ２１１では、ポイント補充情報の命令書を暗号化し、これをセキュリティＩＤと共にポイント補充指示情報として、図６の（５）に示すようにユーザ端末５０に送る。このユーザ端末５０からプレーヤ１に送られた上記ポイント補充指示情報は、当該プレーヤ１において復号化され、さらにセキュリティＩＤの確認後に、ポイント情報格納メモリ２８へのポイント情報の補充と、ポイント使用情報格納メモリ２９からの上記先に連絡した著作権情報等の権利者情報の削除とが行われる。

【００４８】次に、ディジタルコンテンツの鑑賞に伴ってユーザから徴収した課金代金、すなわちポイントの使用情報に応じてユーザの口座から引き落とされることになる代金の分配の手順では、先ず図７の（１）のようにユーザ側２００に対して代金振り込み依頼が金融機関２２０からなされる。このとき、ユーザ側２００の口座に十分な残高がある場合には、特に代金振り込み依頼はなされず、口座に十分な残高がない場合には、図７の（２）のようにユーザ側２００から金融機関２２０に対して代金の振り込みがなされる。

【００４９】金融機関２２０は、所定の手数料を差し引いて、図７の（３）のように、ユーザ側２００から受け取った代金を管理センタ２１１に対して送金する。すなわち管理センタ２１１では、金融機関２２０から送金された上記代金から、コンテンツ加工料と金融手数料とシステム管理費等を徴収する。また、当該管理センタ２１１は、先に使用されたポイントに応じた著作権料を、図７の（４）のようにコンテンツプロバイダ２４０に対して支払うと共に、仮想店舗２３０に対しては図７の（５）のように店舗手数料を支払う。上記著作権料を受け取ったコンテンツプロバイダ２４０は著作権料を各著作権者に支払い、上記店舗手数料を受け取った仮想店舗２３０は仮想店舗毎の手数料を各仮想店舗に対して支払う。

【００５０】このように、ユーザ側２００から支払われた代金は、前記ポイント使用情報に基づいて、著作権料と店舗手数料とコンテンツ加工手数料と決済手数料とシステム管理手数料とに分配され、上記著作権料はコンテンツプロバイダ２４０に、上記店舗手数料は上記仮想店舗２３０に、コンテンツ加工手数料はシステム管理会社２１０に、決済手数料はシステム管理会社と金融機関２２０に、システム管理手数料はシステム管理会社２１０に支払われる。

【００５１】ここで、本実施の形態のシステム間でのデータ送受、すなわち管理センタ２１１とプレーヤ１との間のデータ送受の際には、データ通信の安全性を確保するために、通信するデータの暗号化及び復号化が行われる。本発明実施の形態では、暗号化及び復号化の方式として共通鍵暗号方式及び公開鍵暗号方式の何れにも対応可能となっている。

【００５２】本発明の実施の形態では、上記ディジタルコンテンツ、上記ポイント使用情報、ポイント情報、メッセージやセキュリティＩＤ、その他の各種情報の伝送の際の暗号方式としては、処理速度の点から共通鍵暗号方式を採用している。これら各種情報の暗号化及び復号化に使用する共通鍵は、それぞれ各情報に対応して異なるものである。前記図２のプレーヤ１では、管理センタ２１１から伝送されてくる暗号化された情報の復号化に使用する共通鍵が前記共通鍵保管メモリ２２に保管され、この共通鍵保管メモリ２２に保管している共通鍵を用いて、前記共通暗号復号回路２４が、上記管理センタ２１１からの暗号化された情報の復号化を行う。

【００５３】一方、上記各種情報の暗号化や復号化に使用する上記共通鍵の伝送の際の暗号方式としては、前記プレーヤ１の固有の鍵であるプレーヤ固有鍵が何れの方式に対応しているかによって採用される暗号方式が変わるものである。すなわち、上記プレーヤ固有鍵が共通鍵暗号方式に対応している場合、上記共通鍵は当該プレーヤ固有鍵を用いて暗号化され、また当該暗号化された共通鍵は上記プレーヤ固有鍵を用いて復号化されることになる。これに対して、上記プレーヤ固有鍵が公開鍵暗号方式に対応している場合、上記共通鍵の暗号化には相手先の公開鍵が用いられ、暗号化された上記共通鍵の復号化にはそれぞれ復号化を行う側の秘密鍵が用いられる。

【００５４】例えば上記プレーヤ１から管理センタ２１１に上記共通鍵（例えば後述するセッション鍵）が送られる場合において、上記プレーヤ固有鍵が共通鍵暗号方式に対応しているときには、上記プレーヤ１では通信用鍵保管メモリ２１が保管しているプレーヤ固有鍵を用いて上記共通鍵暗号復号回路２４が上記共通鍵を暗号化し、管理センタ２１１では当該管理センタ２１１が保管しているプレーヤ固有鍵を用いて、上記暗号化されてる共通鍵の復号化を行う。同じく、上記プレーヤ１から管

理センタ２１１に上記共通鍵が送られる場合において、例えば上記プレーヤ固有鍵が公開鍵暗号方式に対応しているときには、上記プレーヤ１の通信用用鍵保管メモリ２１が保管している管理センタ２１１の公開鍵にて上記公開鍵暗号復号回路２０が上記共通鍵を暗号化し、管理センタ２１１では当該管理センタ２１１が保管している秘密鍵を用いて、上記暗号化されてる共通鍵の復号化を行う。

【００５５】逆に、例えば上記管理センタ２１１からプレーヤ１に上記共通鍵（例えばコンテンツ鍵）が送られる場合において、上記プレーヤ固有鍵が共通鍵暗号方式に対応しているときには、上記管理センタ２１１が保管しているプレーヤ固有鍵にて上記共通鍵が暗号化され、プレーヤ１では上記通信用鍵保管メモリ２１にて保管しているプレーヤ固有鍵を用いて、前記共通暗号復号回路２４が上記暗号化されてる共通鍵の復号化を行う。同じく、上記管理センタ２１１からプレーヤ１に上記共通鍵が送られる場合において、例えば上記プレーヤ固有鍵が公開鍵暗号方式に対応しているときには、上記管理センタ２１１が保管しているプレーヤ１の公開鍵にて上記共通鍵が暗号化され、プレーヤ１では上記通信用鍵保管メモリ２１にて保管しているプレーヤ固有鍵すなわち秘密鍵を用いて、前記公開暗号復号回路２０が上記暗号化されてる共通鍵の復号化を行う。

【００５６】上述したようなプレーヤ固有鍵自身の暗号方式は、当該プレーヤ固有鍵の配送（システム管理会社２１０からプレーヤ１への配送）が容易か否かによって決定されている。すなわち、コスト的には共通鍵暗号方式の方が有利であるので、プレーヤ固有鍵の配送が容易であれば共通鍵暗号方式を採用するが、当該プレーヤ固有鍵の配送が困難であるときにはコスト高であるが公開鍵暗号方式を採用する。プレーヤ固有鍵をハードウェアに実装する場合には共通鍵暗号方式を、ソフトウェアに実装する場合には公開鍵暗号方式を採用する。

【００５７】以下、本発明の実施の形態では、プレーヤ固有鍵自身の暗号方式としてソフトウェアに実装する場合の互換性を考慮して、上記公開鍵暗号方式を採用する例を挙げて説明することにする。すなわち、上記管理センタ２１１とプレーヤ１との間で前記共通鍵の伝送が行われる場合において、上記プレーヤ１側で共通鍵（セッション鍵）が暗号化されるときには管理センタ２１１の公開鍵を用いて暗号化がなされ、管理センタ２１１では上記プレーヤ固有鍵（すなわち秘密鍵）を用いて上記暗号化されてる共通鍵の復号化を行う。逆に、上記管理センタ２１１側で共通鍵（コンテンツ鍵）が暗号化されるときには、プレーヤの公開鍵にて暗号化がなされ、プレーヤ１では上記プレーヤ固有鍵（すなわち秘密鍵）を用いて上記暗号化されてる共通鍵の復号化を行う。

【００５８】前述したような各手順と暗号方式を用いて運用されるシステムを構成する上記プレーヤ１とユーザ端末５０と管理センタ２１１の実際の動作を、以下に順番に説明する。

【００５９】先ず、上述したポイント補充すなわちポイント購入時のプレーヤ１、ユーザ端末５０、管理センタ１０における処理の流れについて、図８から図１１を用い、前記図２及び図３を参照しながら説明する。

【００６０】図８には、ポイントを購入する際のプレーヤ１における処理の流れを示している。

【００６１】この図８において、ステップＳＴ１では、ユーザ端末５０すなわちパーソナルコンピュータに予めインストールされているポイント購入用のソフトウェアの立ち上げが行われ、この間のプレーヤ１のコントローラ１６は、当該ポイント購入用のソフトウェアが立ち上がるまで待っている。

【００６２】上記ポイント購入用のソフトウェアが立ち上がると、ステップＳＴ２にて、プレーヤ１のコントローラ１６は、上記ユーザ端末５０に入力された情報を、当該ユーザ端末５０から受信する。このときのユーザ端末５０に入力される情報とは、上記ポイント購入用のソフトウェアに従って、上記ユーザ端末５０を操作するユーザに対して当該ユーザ端末５０から入力要求がなされるものであり、例えばパスワードや購入したいポイント情報数等の情報である。

【００６３】これらユーザ端末５０からの情報は、プレーヤ１のＰＣ用インターフェース端子３及び当該プレーヤ１内に１チップ化された集積回路１０の端子１２を介して、コントローラ１６に受信される。当該ユーザ端末５０からの情報を受信したコントローラ１６は、ステップＳＴ３にて、当該プレーヤ１の集積回路１０内のパスワード格納メモリ１４が格納するパスワードと、上記受信した情報中のパスワードとの比較を行い、上記受信パスワードが正しいかどうかの確認を行う。

【００６４】上記パスワードが正しいと確認したコントローラ１６は、ステップＳＴ４にて、ポイントを購入したい旨の情報（ポイント購入の主旨）と購入したいポイント情報数その他の情報を生成すると同時に、セキュリティＩＤ発生回路１９からセキュリティＩＤを発生させ、次のステップＳＴ５にてこれらの情報を共通暗号復号回路２４にて暗号化させる。コントローラ１６は、次にステップＳＴ６にて、ユーザＩＤ格納メモリ２３からユーザＩＤを読み出し、当該ユーザＩＤを上記暗号化した情報に付加し、さらに、ステップＳＴ７にて、当該ユーザＩＤを付加して作成したデータを上記端子１２及びＰＣ用インターフェース端子３を介してユーザ端末５０に転送する。このユーザ端末５０からは、上記作成データが管理センタ２１１に送られることになる。

【００６５】このとき、上記作成データの暗号化には前述したように共通鍵暗号方式が採用されているため、当該作成データの伝送に先立ち、共通鍵の生成が行われる。このため、上記コントローラ１６では、上記共通鍵

として、例えば乱数発生手段であるセキュリティＩＤ発生回路１９からセッション鍵を発生させる。また、この共通鍵（セッション鍵）は、上記作成データの伝送に先だって、プレーヤ１から管理センタ２１１に対して送られることになる。ここで、当該共通鍵は前述のように公開鍵暗号方式にて暗号されるものであるため、上記コントローラ１６では、上記共通鍵であるセッション鍵を公開暗号復号回路２０に送ると同時に、通信用鍵保管メモリ２１に予め保管されている管理センタ２１１の公開鍵を取り出して上記公開暗号復号回路２０に送る。これにより当該公開暗号復号回路２０では、上記管理センタ２１１の公開鍵を用いて上記共通鍵（セッション鍵）の暗号化が行われる。このようにして暗号化されたセッション鍵はユーザＩＤと共に、上記作成データの伝送に先だって管理センタ２１１に送られている。

【００６６】なお、前述したように、ポイント情報の要求と共にポイント使用情報の転送も行う場合、コントローラ１６は、ポイント使用情報格納メモリ２９から前記権利者情報等を含むポイント使用情報を読み出し、これらも上記共通暗号復号回路２６に送って暗号化させる。この暗号化したポイント使用情報は、上記作成データと共に伝送される。また、ポイント使用情報の転送と同時に、ポイント情報の残高をも同様にして転送することも可能である。

【００６７】その後、コントローラ１６は、ステップＳＴ８にて、ユーザ端末５０を通して管理センタ２１１から送られてきた暗号化されているデータを受信する。この管理センタ２１１から送られてきたデータは、先に当該プレーヤ１から転送した上記購入したいポイント情報数に応じたポイント情報とセキュリティＩＤ等の情報が、上記セッション鍵と同じ共通鍵を用いて暗号化されたデータである。

【００６８】コントローラ１６は、上記管理センタ２１１からのデータを受信すると、ステップＳＴ９にて、当該データを上記共通暗号復号回路２４に送ると共に、先に発生して共通鍵保管メモリ２２に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路２４に送る。当該共通暗号復号回路２４では、上記共通鍵を用いて上記管理センタ２１１からの暗号化されたデータを復号化する。

【００６９】次に、上記コントローラ１６は、ステップＳＴ１０にて、上記復号化されたデータのセキュリティＩＤを、上記セキュリティＩＤ発生回路１９からのセキュリティＩＤとの比較によって確認し、その確認後、ステップＳＴ１１にて、上記ポイント情報格納メモリ２８に格納されていたポイント情報を、上記新たに送られてきたポイント情報にて修正する。

【００７０】上記ポイント情報の修正等の処理が終了すると、コントローラ１６は、ステップＳＴ１２にて、処理完了のサインを生成し、上記共通鍵保管メモリ２２から読み出した共通鍵と共に上記共通暗号復号回路２４に送り、当該共通暗号復号回路２４にて暗号化させる。その後、コントローラ１６は、ステップＳＴ１３にて当該暗号化された処理完了のサインを、端子１２及び３を介してユーザ端末５０に転送し、管理センタ２１１に送る。

【００７１】以上により、ポイント購入の際のプレーヤ１における処理の流れが終了する。

【００７２】次に、上記ポイント購入時のユーザ端末５０における処理の流れを、図９を用いて説明する。

【００７３】この図９において、ユーザ端末５０は、ステップＳＴ２１にて、ポイント購入用のソフトウェアの立ち上げを行う。当該ポイント購入用ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ２２にて、上記ポイント購入用のソフトウェアに従い当該ユーザ端末５０を操作するユーザに対して上述したパスワードや購入したいポイント数等の情報の入力要求を行い、ユーザからこれらの情報が入力されると、当該入力された情報を前記図８のステップＳＴ２のように上記プレーヤ１に転送する。

【００７４】次に、ユーザ端末５０は、ステップＳＴ２３にて、上記プレーヤ１から前記図８のステップＳＴ７のように作成されたデータを受信すると、ステップＳＴ２４にて、当該プレーヤ１から転送されたデータを、予め登録されているアドレスすなわち管理センタ２１１へ転送する。

【００７５】上記データの転送を行った後のユーザ端末５０は、管理センタ２１１からの返送を待ち、管理センタ２１１からのデータ返送があると、ステップＳＴ２５にて当該管理センタ２１１からのデータをそのままプレーヤ１に転送する。

【００７６】当該ユーザ端末５０は、ステップＳＴ２６にて、上記プレーヤ１から前記図８のステップＳＴ１３のように処理完了のサインを受信すると、当該ポイント購入等の処理が終了したことをユーザに知らせるために、ステップＳＴ２７にて処理完了のサインをディスプレイに表示し、ユーザに確認させる。

【００７７】その後、当該ユーザ端末５０は、上記プレーヤ１から送られてきた処理完了のサインの暗号文を管理センタ２１１に転送する。

【００７８】以上により、ポイント購入の際のユーザ端末５０における処理の流れが終了する。

【００７９】次に、ポイント購入時の管理センタ２１１における処理の流れを、図１０を用いて説明する。

【００８０】この図１０において、管理センタ２１１は、ステップＳＴ３１のように、コントロール機能部１３１にて全体が制御される管理機能ブロック１３０の通信機能部１３３によって、前記図８のステップＳＴ７及び図９のステップＳＴ２４のようにユーザ端末５０を介して転送されたプレーヤ１からの上記暗号化されたデー

タを受信する。このデータを受信すると、管理センタ２１１のユーザ管理機能ブロック１１０は、ステップＳＴ３２のように、コントロール機能部１１１の制御の元で、当該受信したデータに添付されたユーザＩＤに基づいて、データベース部１１２から共通鍵を入手すると共にセキュリティＩＤ発生機能部１１６からセキュリティＩＤを入手する。

【００８１】なお、この時の共通鍵は、前記プレーヤ１から予め送られてきている前記セッション鍵であり、このセッション鍵は前述のように公開鍵暗号方式にて暗号化されて送られてきたものである。したがって、この暗号化されているセッション鍵の復号時には、当該管理センタ２１１のユーザ管理機能ブロック１１０において、当該管理センタ２１１の公開鍵暗号方式の秘密鍵が取り出され、この秘密鍵と上記暗号化されているセッション鍵とが通信文暗号／復号機能部１１４に送られる。当該通信文暗号／復号機能部１１４では、上記管理センタ２１１の公開鍵を用いて上記暗号化されたセッション鍵の復号化が行われる。このようにして得られたセッション鍵（共通鍵）が上記データベース部１１２に格納されている。

【００８２】上記データベース部１１２から上記ユーザＩＤに対応する共通鍵を入手すると共にセキュリティＩＤ発生機能部１１６からセキュリティＩＤを入手すると、ステップＳＴ３３に示すように、管理センタ２１１のユーザ管理機能ブロック１１０の通信文暗号／復号機能部１１４において、上記共通鍵を用いて、上記プレーヤ１からの上記暗号化されたデータの復号化を行い、さらにコントロール機能部１１１において、当該復号化したデータ中のセキュリティＩＤと上記セキュリティＩＤ発生機能部１１６から読み出したセキュリティＩＤとの比較によって、アクセスしてきたユーザ側２００（プレーヤ１）が正当な使用者であるかどうかの内容確認を行う。

【００８３】上記アクセス元の正当性を確認した管理センタ２１１では、ステップＳＴ３４のように、ユーザ管理機能ブロック１１０のポイント発生機能部１１３にて、上記ユーザ端末５０から送られてきたデータの内容に応じたポイント情報の発行を行い、また、決済請求機能部１１７にて、ユーザの決済機関（金融機関２２０）への請求準備を行う。

【００８４】さらに、管理センタ２１１は、ステップＳＴ３５のように、例えばコントロール機能部１１１において、プレーヤ１からのポイント情報の残高とポイント使用情報に不正が無いことを確認し、後の処理のために情報のまとめを行う。すなわち、ポイント情報の残高と実際に使用したポイント情報の数とから不正な使用がないかどうかの確認とまとめとを行う。なお、この確認とまとめは、必ず行わなければならないものではないが、望ましくは行った方が良い。

【００８５】管理センタ２１１のユーザ管理機能ブロック１１０ではまた、上記ステップＳＴ３５の処理の後、ステップＳＴ３６のように、セキュリティＩＤ発生機能部１１５において上記プレーヤ１（ユーザ）への新たなセキュリティＩＤを例えば乱数発生に基づいて算出し、さらに、例えばコントロール機能部１１０にて、上記セキュリティＩＤを上記ポイント情報と共に暗号化する。このときの暗号化も前記プレーヤ１から予め送られてきている前記セッション鍵（共通鍵）を用いて行う。

【００８６】上記暗号化が終了すると、管理センタ２１１の管理機能ブロック１３０の通信機能部１３３では、コントロール機能部１３１の制御の元、上記暗号化したデータを前記図９のステップＳＴ２５及び図８のステップＳＴ８のようにユーザ端末５０を介してプレーヤ１に転送する。

【００８７】その後、管理センタ２１１の通信機能部１３３において、ステップＳＴ３８のように、前記図９のステップＳＴ２８に示したユーザ端末５０からの処理完了サインを受信して復号化すると、管理センタ２１１のユーザ管理機能ブロック１１０の決済請求機能部１１７では、ステップＳＴ３９のように、当該処理完了サインに基づいて金融機関２２０に決済を請求する。この金融機関２２０に対する決済請求は、管理機能ブロック１３０の通信機能部１３２から行われる。

【００８８】以上により、ポイント購入の際の管理センタ２１１における処理の流れが終了する。

【００８９】上述した図８から図１０の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図１１に示すように表すことができる。

【００９０】すなわちこの図１１において、入力情報転送Ｔ１では、前記図８のステップＳＴ２及び図９のステップＳＴ２２のように、ユーザ端末５０からプレーヤ１に対して、前記パスワードやポイント数等の入力情報が転送される。

【００９１】作成データ転送Ｔ２では、前記図８のステップＳＴ７及び図９のステップＳＴ２３のように、プレーヤ１からユーザ端末５０に対して、前記プレーヤ１にて作成したデータが転送される。また、データ転送Ｔ３では、前記図９のステップＳＴ２４及び図１０のステップＳＴ３１のように、ユーザ端末５０から管理センタ２１１に対して、前記プレーヤ１が作成したデータが転送される。

【００９２】データ転送Ｔ４では、前記図１０のステップＳＴ３７及び図９のステップＳＴ２５のように、管理センタ２１１からユーザ端末５０に対して、管理センタ２１１にて暗号化したデータが転送される。また、転送Ｔ５では、前記図９のステップＳＴ２５及び図８のステップＳＴ８のように、管理センタ２１１からのデータをユーザ端末５０がそのままプレーヤ１に転送される。

【００９３】処理完了サイン転送Ｔ６では、前記図８のステップＳＴ１３及び図９のステップＳＴ２６のように、プレーヤ１からの処理完了サインがユーザ端末５０に転送される。さらに、処理完了サイン暗号文転送では、前記図９のステップＳＴ２８及び図１０のステップＳＴ３８のように、プレーヤ１からの暗号化された処理完了サインが管理センタ２１１に転送される。

【００９４】次に、上述したディジタルコンテンツの入手時のプレーヤ１、ユーザ端末５０、管理センタ２１１における処理の流れについて、図２及び図３を参照しながら、図１２から図１５を用いて説明する。

【００９５】図１２には、ディジタルコンテンツの入手時のプレーヤ１における処理の流れを示している。

【００９６】この図１２において、コントローラ１６は、ステップＳＴ４１のように、ユーザ端末５０すなわちパーソナルコンピュータに予めインストールされているディジタルコンテンツ入手用のソフトウェアの立ち上げが行われるまで待っている。

【００９７】上記ディジタルコンテンツ入手用のソフトウェアが立ち上がると、コントローラ１６は、ステップＳＴ４２のように、ユーザ端末５０を介して管理センタ２１１からディジタルコンテンツを含むデータを受信する。このときユーザ端末５０から端子３及び１２を介して受信するデータは、前述したようにコンテンツ鍵（コンテンツ毎に異なる共通鍵）で暗号化されたディジタルコンテンツと、当該ディジタルコンテンツに対応するコンテンツＩＤとを少なくとも有してなる。したがって、この暗号化されたディジタルコンテンツを使用するには、コンテンツ鍵を管理センタ２１１から入手しなければならない。このコンテンツ鍵の入手の方法については後述する。

【００９８】このユーザ端末５０からのデータを受信したコントローラ１６は、このデータすなわち暗号化されたディジタルコンテンツを、集積回路１０の端子１１を介し、記憶メディア用Ｉ／Ｏ端子４に接続されている記憶メディアに格納する。なお、この記憶メディアとしては、書き換え可能な光ディスクや半導体メモリ等の各種の記憶媒体が考えられるが、ランダムアクセス可能なものが望ましい。

【００９９】以上により、ディジタルコンテンツの入手時のプレーヤ１における処理の流れが終了する。

【０１００】次に、ディジタルコンテンツの入手時のユーザ端末５０における処理の流れを、図１３を用いて説明する。

【０１０１】この図１３において、ユーザ端末５０は、ステップＳＴ５１にて、ディジタルコンテンツ入手用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ５２にて、上記ディジタルコンテンツ入手用のソフトウェアに従い、予め登録されているアドレスの管理センタ２１１にアクセスする。

【０１０２】このとき、当該管理センタ２１１は、前記仮想店舗２３０を用いて複数のディジタルコンテンツを展示している。ユーザ端末５０からは、ステップＳＴ５３にて、この仮想店舗２３０に展示されている複数のディジタルコンテンツのなかから、ユーザの選択操作に応じた所望のディジタルコンテンツが指定される。すなわち、ユーザ端末５０は、ステップＳＴ５４のように、仮想店舗２３０に展示されたディジタルコンテンツの中の所望のディジタルコンテンツを指定するためのコンテンツの指定情報を管理センタ２１１に送信する。

【０１０３】ステップＳＴ５５のように、上記コンテンツ指定情報に応じて管理センタ２１１から返送されたデータ、すなわち前記暗号化されたディジタルコンテンツ及びコンテンツＩＤからなるデータを受信すると、当該ユーザ端末５０は、ステップＳＴ５６のように、内部の例えばハードディスクやメモリ等の格納手段に上記データを一旦格納する。

【０１０４】その後、ユーザ端末５０は、当該格納したデータ（暗号化されたディジタルコンテンツ及びコンテンツＩＤ）を、前記図１２のステップＳＴ４２のようにプレーヤ１に転送する。

【０１０５】以上により、ディジタルコンテンツの入手時のユーザ端末５０における処理の流れが終了する。

【０１０６】次に、ディジタルコンテンツ入手時の管理センタ２１１における処理の流れを、図１４を用いて説明する。

【０１０７】ここで、図３に示す管理センタ２１１は、前述した仮想店舗２３０に複数のコンテンツを展示させている。具体的には、管理センタ２１１ののコンテンツ管理機能ブロック１００において、前記仮想店舗２３０を生成しており、この仮想店舗２３０に上記複数のディジタルコンテンツの展示を行っている。

【０１０８】このように仮想店舗２３０にディジタルコンテンツを展示している状態で、図１４のステップＳＴ６１のように、前記図１３のステップＳＴ５４にてユーザ端末５０からコンテンツ指定情報を受信する。

【０１０９】当該ユーザ端末５０から上記コンテンツ指定情報を受信すると、コンテンツ管理機能ブロック１００のコントロール機能部１０１は、このコンテンツ指定情報を管理機能ブロック１３０に送る。管理機能ブロック１３０のコントロール機能部１３１は、上記コントロール管理機能ブロック１００から受け取ったコンテンツ指定情報を、権利者用の通信機能部１３４を通して、前記コンテンツプロバイダ２４０に転送する。これにより当該コンテンツプロバイダ２４０からは、上記コンテンツ指定情報にて要求されたディジタルコンテンツが転送されてくる。上記コンテンツプロバイダ２４０から入手したディジタルコンテンツは、管理機能ブロック１３０からコンテンツ管理機能ブロック１００に送られ、この

コンテンツ暗号・圧縮化機能部１０４に入力される。このとき、コントロール機能部１０１は、コンテンツ鍵・ＩＤ発生機能部１０３にて発生されてデータベース１０２に格納されているコンテンツ鍵を、上記コンテンツ暗号・圧縮化機能部１０４に送る。このコンテンツ暗号・圧縮化機能部１０４では、上記ディジタルコンテンツに対して上記コンテンツ鍵を用いた暗号化を施し、さらに所定の圧縮処理を施す。コントロール機能部１０１は、上記暗号化及び圧縮処理されたディジタルコンテンツに対して、データベース１０２から取り出したコンテンツＩＤを付加し、管理機能ブロック１３０に送る。なお、ディジタルコンテンツがオーディオ信号である場合の所定の圧縮処理としては、例えば近年製品化されているいわゆるＭＤ（ミニディスク：商標）にて使用されている技術である、いわゆるＡＴＲＡＣ（Adaptive TRansform Acoustic Coding）のように、人間の聴覚特性を考慮してオーディオデータを高能率圧縮する処理を一例とした挙げることができる。

【０１１０】その後、図１４のステップＳＴ６２に示すように、管理機能ブロック１３０のコントロール部１３１は、ユーザ端末との通信機能部１３３を通して、上記暗号化及び圧縮処理されてコンテンツＩＤが付加されたディジタルコンテンツを、上記ユーザ端末５０に送信する。

【０１１１】ディジタルコンテンツ入手時の管理センタ２１１における処理の流れは以上である。

【０１１２】上述した図１２から図１４の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図１５に示すように表すことができる。

【０１１３】すなわちこの図１５において、入力情報転送Ｔ１１では、前記図１３のステップＳＴ５４のように、ユーザ端末５０から管理センタ２１１に対して、前記コンテンツ指定情報が転送される。コンテンツ転送Ｔ１２では、管理センタ２１１から、前記図１４のステップＳＴ６２のように、暗号化されたディジタルコンテンツとコンテンツＩＤがユーザ端末５０に転送される。

【０１１４】コンテンツ転送Ｔ１３では、前記図１３のステップＳＴ５７及び図１２のステップＳＴ４２のように、ユーザ端末５０に一旦格納された上記暗号化されたディジタルコンテンツとコンテンツＩＤがプレーヤ１に転送される。

【０１１５】次に、上述したディジタルコンテンツを使用する際に必要となるコンテンツ鍵とその使用条件の入手時のプレーヤ１、ユーザ端末５０、管理センタ２１１における処理の流れについて、図２及び図３を参照しながら、図１６から図１９を用いて説明する。

【０１１６】図１６には、コンテンツ鍵及び使用条件の入手時のプレーヤ１における処理の流れを示している。

【０１１７】この図１６のステップＳＴ７１では、プレーヤ１のコントローラ１６において、ユーザ端末５０に予めインストールされているコンテンツ鍵及び使用条件入手用のソフトウェアの立ち上げが行われるまで待っている。

【０１１８】上記ユーザ端末５０の上記コンテンツ鍵及び使用条件入手用のソフトウェアが立ち上がると、当該ソフトウェアに従ってユーザ端末５０に入力された情報が、ステップＳＴ７２のように、前記ＰＣ用インターフェース端子３及び集積回路１０の端子１２を介して受信される。このときの上記ユーザ端末５０から供給される入力情報は、鑑賞したいディジタルコンテンツの暗号化を解くのに必要なコンテンツ鍵を要求するための情報である。なお、この例では、上記コンテンツ鍵の要求情報として、このコンテンツ鍵を使用するディジタルコンテンツの指定情報を用いている。

【０１１９】このコンテンツ指定情報を上記ユーザ端末５０から受信したコントローラ１６は、ステップＳＴ７３にて、当該コンテンツ指定情報にて指定されたディジタルコンテンツのＩＤと、セキュリティＩＤ発生回路１９からのセキュリティＩＤとを作成し、この作成したデータを共通暗号復号回路２４にて暗号化させる。また、コントローラ１６は、当該作成したデータにユーザＩＤ格納メモリ２３から読み出したユーザＩＤを付加し、上記端子１２及びＰＣ用インターフェース端子３を介してユーザ端末５０に転送する。このユーザ端末５０からは、上記作成データが管理センタ２１１に送られることになる。

【０１２０】このときの作成データの暗号化にも、前述したように共通鍵暗号方式が採用されているため、当該作成データの伝送に先立ち、共通鍵の生成が行われる。このため、上記コントローラ１６では、上記共通鍵として、例えば乱数発生手段であるセキュリティＩＤ発生回路１９からセッション鍵を発生させる。また、この共通鍵（セッション鍵）は、上記作成データの伝送に先だって、プレーヤ１から管理センタ２１１に対して送られることになる。当該共通鍵は、前述のように公開鍵暗号方式にて暗号されるものであるため、上記コントローラ１６では、上記共通鍵であるセッション鍵を公開暗号復号回路２０に送ると同時に、通信用鍵保管メモリ２１に予め保管されている管理センタ２１１の公開鍵を取り出して上記公開暗号復号回路２０に送る。これにより当該公開暗号復号回路２０では、上記管理センタ２１１の公開鍵を用いて上記共通鍵（セッション鍵）の暗号化が行われる。このようにして暗号化されたセッション鍵が、上記作成データの伝送に先だって管理センタ２１１に送られている。

【０１２１】その後、コントローラ１６は、ステップＳＴ７５にて、後述するようにユーザ端末５０を介して管理センタ２１１から送付されてきた暗号化されたデータを受信する。このときの管理センタ２１１から送られて

きたデータは、後述するように上記コンテンツ鍵と使用条件とセキュリティＩＤ等が暗号化されたものである。

【０１２２】上記管理センタ２１１からの暗号化されたデータを受信すると、プレーヤ１では、ステップＳＴ７６のように、上記暗号化されたデータを復号化すると共にそのデータの正当性の確認を行う。すなわち、コントローラ１６は、上記復号化されたデータのセキュリティＩＤを、上記セキュリティＩＤ発生回路１９からのセキュリティＩＤとの比較によって確認することによる正当性の評価を行う。

【０１２３】ここで、コンテンツ鍵については後述するように公開鍵暗号方式にて暗号化がなされ、使用条件及びセキュリティＩＤについては共通鍵暗号方式にて暗号化がなされている。したがって、当該暗号化されているコンテンツ鍵を復号化するには、公開鍵暗号方式の秘密鍵が必要であり、本実施の形態のプレーヤ１では前述したようにプレーヤ固有鍵を秘密鍵として使用することにしているので、当該プレーヤ固有鍵が通信用鍵保管メモリ２１から取り出される。このプレーヤ固有鍵は、上記暗号化されたコンテンツ鍵と共に公開暗号復号回路２０に送られる。この公開暗号復号回路２０では、上記暗号化されているコンテンツ鍵を上記プレーヤ固有鍵を用いて復号化する。このように復号化されたコンテンツ鍵は、共通鍵保管メモリ２２に保管される。一方、上記共通鍵暗号方式にて暗号化されている使用条件とセキュリティＩＤを復号化する場合には、これらのデータを上記共通暗号復号回路２４に送ると共に、先に発生して共通鍵保管メモリ２２に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路２４に送る。当該共通暗号復号回路２４では、上記共通鍵を用いて上記使用条件とセキュリティＩＤを復号化する。このように復号化された使用条件は、ポイント使用情報格納メモリ２９に格納される。なお、ここで重要なのは、当該復号化されたコンテンツ鍵・使用条件は、当該プレーヤ１の外部、具体的には図２の集積回路１０内に設けられたコントローラ１６や共通鍵保管メモリ２２、ポイント使用情報格納メモリ２９から外部には取り出されないことである。

【０１２４】この正当性の確認後、コントローラ１６は、ステップＳＴ７７のように、上記復号したコンテンツ鍵を上記コンテンツＩＤと共に上記共通鍵保管メモリ２２に格納させる。

【０１２５】その後、コントローラ１６は、ステップＳＴ７８にて、上記コンテンツ鍵を入手した旨を示すメッセージを作成し、このメッセージを前述同様に共通鍵暗号復号回路２４に送り、予め発生して共通鍵保管メモリ２２に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路２４に送る。当該共通暗号復号回路２４では、上記共通鍵を用いてメッセージを暗号化する。

【０１２６】当該メッセージの暗号化が終了すると、コントローラ１６は、ステップＳＴ７９のように、この暗号化されたメッセージを端子１２及び３を介してユーザ端末５０に送信する。この暗号化されたメッセージは、その後、管理センタ２１１に転送させる。

【０１２７】以上により、コンテンツ鍵・使用条件入手時のプレーヤ１における処理の流れが終了する。

【０１２８】次に、コンテンツ鍵・使用条件入手時のユーザ端末５０における処理の流れを、図１７を用いて説明する。

【０１２９】この図１７において、ユーザ端末５０は、ステップＳＴ８１にて、コンテンツ鍵・使用条件入手用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ８２にて、上記ソフトウェアに従い当該ユーザ端末５０を操作するユーザに対して、希望のコンテンツの指定入力要求を行い、ユーザからコンテンツの指定がなされると、その指定情報を生成する。ユーザ端末５０は、上記ステップＳＴ８３にて、上記コンテンツの指定情報をプレーヤ１に対して送信する。

【０１３０】次に、ユーザ端末５０は、ステップＳＴ８４にて、前記図１６のステップＳＴ７４のように上記プレーヤ１にて作成されて転送されたデータを受信すると、ステップＳＴ８５にて、当該プレーヤ１から転送されたデータを、予めアドレスが登録されている管理センタ２１１へ転送する。

【０１３１】上記管理センタ２１１に対してデータの転送を行った後のユーザ端末５０は、管理センタ２１１からの返送を待ち、ステップＳＴ８６にて、管理センタ２１１から上記コンテンツＩＤで指定されたコンテンツ鍵・使用条件とセキュリティＩＤ等が暗号化されたデータの返送があると、ステップＳＴ８７にて当該管理センタ２１１からのデータをそのままプレーヤ１に転送する。

【０１３２】上記プレーヤ１に対してデータの転送を行った後のユーザ端末５０は、プレーヤ１からの返送を待ち、ステップＳＴ８８にて、プレーヤ１から前記図１６のステップＳＴ７９のように、上記コンテンツ鍵を入手した旨の暗号化されたメッセージの返送があると、ステップＳＴ８９にて当該ユーザ端末５０に接続されたディスプレイ装置に対して上記コンテンツ鍵入手が完了した旨の表示を行ってユーザに知らせる。

【０１３３】その後、上記プレーヤ１から返送された上記暗号化されたメッセージを、ステップＳＴ９０にて、管理センタ２１１に送付する。

【０１３４】以上により、コンテンツ鍵・使用条件入手時のユーザ端末５０における処理の流れが終了する。

【０１３５】次に、コンテンツ鍵・使用条件入手時の管理センタ２１１における処理の流れを、図１８を用いて説明する。

【０１３６】この図１８において、管理センタ２１１のユーザ端末との通信機能部１３３は、ステップＳＴ９１にて、前記図１６のステップＳＴ７４及び図１７のステ

ップＳＴ８５のようにユーザ端末５０にてを介してプレーヤ１から送信されてきたコンテンツＩＤ，ユーザＩＤ、メッセージ、セキュリティＩＤの暗号化データを受信する。この受信したデータは、ユーザ管理機能ブロック１１０に送られる。

【０１３７】当該ユーザ管理機能ブロック１１０のコントロール機能部１１１は、上記受信した暗号化データに付加されたユーザＩＤに基づいて、当該暗号化を解くための共通鍵をデータベース部１１２から取り出し、通信文暗号・復号機能部１１４ではこの共通鍵を用いて上記暗号化データを復号する。また、コントロール機能部１１１は、データベース部１１２から読み出したユーザＩＤとセキュリティＩＤ発生機能部１１６からのセキュリティＩＤとを用いて、上記受信して復号化したデータの正当性を確認する。

【０１３８】なお、この時の共通鍵は、前記プレーヤ１から予め送られてきている前記セッション鍵であり、このセッション鍵は前述のように公開鍵暗号方式にて暗号化されて送られてきたものである。したがって、この暗号化されているセッション鍵の復号時には、前述同様に当該管理センタ２１１において、管理センタ２１１の公開鍵暗号方式の秘密鍵が取り出され、当該通信文暗号／復号機能部１１４にて上記暗号化されているセッション鍵が秘密鍵を用いて復号化される。このようにして得られたセッション鍵（共通鍵）が上記データベース部１１２に格納されている。

【０１３９】上記受信したデータの正当性を確認すると、コントロール機能部１１１は、コンテンツ管理機能ブロック１００に対して上記コンテンツＩＤにて指定されたコンテンツ鍵と使用条件を要求し、当該要求を受けたコンテンツ管理機能ブロック１００のコントロール機能部１０１は、上記コンテンツＩＤにて指定されたコンテンツ鍵と使用条件とをデータベース部１０２から読み出してユーザ管理機能ブロック１１０に転送する。コントロール機能部１１１は、ステップＳＴ９３に示すように、これらコンテンツ鍵と使用条件はセキュリティＩＤと共に通信文暗号／復号機能部１１４に送る。

【０１４０】ここで、コンテンツ鍵については前述した公開鍵暗号方式にて暗号化がなされ、使用条件及びセキュリティＩＤについては前述した共通鍵暗号方式にて暗号化がなされる。したがって、当該コンテンツ鍵を暗号化する時には、前記データベース部１１２からユーザ側２００の公開鍵（プレーヤ１に対応して予め格納されている公開鍵）が上記ユーザＩＤに基づいて取り出されて通信文暗号／復号機能部１１４に送られる。当該通信文暗号／復号機能部１１４では、上記公開鍵を用いて上記コンテンツ鍵を暗号化する。一方、上記使用条件及びセキュリティＩＤを暗号化する時には、上記データベース部１１２から上記ユーザＩＤで指定された共通鍵（セッション鍵）が取り出されて通信文暗号／復号機能部１１４に送られる。このときの通信文暗号／復号機能部１１４では、上記使用条件及びセキュリティＩＤを上記共通鍵を用いて暗号化する。

【０１４１】上記暗号化されたコンテンツ鍵と使用条件及びセキュリティＩＤは、管理機能ブロック１３０に送られ、ステップＳＴ９４のように、ユーザ端末との通信機能部１３３からユーザ端末５０に送信される。このユーザ端末５０に送信されたデータは、前記図１７のステップＳＴ８７及び図１６のステップＳＴ７５のようにユーザ端末５０を介してプレーヤ１に送付されることになる。

【０１４２】その後、管理センタ２１１は、前記図１６のステップＳＴ７９及び図１７のステップＳＴ９０のようにプレーヤ１にて生成されてユーザ端末５０を介して送信された暗号化メッセージの受信を待ち、ステップＳＴ９５のように上記通信機能部１３３が上記プレーヤ１が生成した暗号化メッセージを受信すると、当該管理センタ２１１は、ステップＳＴ９６のように、当該暗号化メッセージを共通鍵で復号化し、その復号メッセージから上記プレーヤ１がコンテンツ鍵と使用条件を入手したことを確認する。

【０１４３】以上により、コンテンツ鍵・使用条件入手時の管理センタ２１１における処理の流れが終了する。

【０１４４】上述した図１６から図１８の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図１９に示すように表すことができる。

【０１４５】すなわちこの図１９において、コンテンツ指定情報転送Ｔ２１では、前記図１７のステップＳＴ８３のように、ユーザ端末５０からプレーヤ１に対して、前記コンテンツ指定情報が転送される。作成データ転送Ｔ２２では、前記のステップＳＴ７４のように、プレーヤ１にて作成されたデータがユーザ端末５０に転送される。作成データ転送Ｔ２３では、当該ユーザ端末５０から上記プレーヤ１にて作成されたデータが管理センタ２１１に転送される。暗号化されたデータ送付Ｔ２４では、前記図１８のステップＳＴ９４のように、管理センタ２１１にて暗号化されたデータがユーザ端末５０に送付され、さらに、暗号化されたデータ送付Ｔ２５では、当該暗号化されたデータがプレーヤ１に送付される。

【０１４６】メッセージ転送Ｔ２６では、前記図１６のステップＳＴ７９のように、コンテンツ鍵入手完了を示すメッセージを暗号化したデータがプレーヤ１からユーザ端末５０に転送され、さらに暗号化されたデータ送付Ｔ２７では、上記プレーヤ１からの暗号化されたメッセージが、ユーザ端末５０から管理センタ２１１に送付される。

【０１４７】次に、上述したようにしてポイント情報とディジタルコンテンツとコンテンツ鍵とを受け取ったプレーヤ１において、ユーザ端末５０を用いてディジタル

コンテンツを実際に鑑賞する際の処理の流れについて、図２を参照しながら図２０を用いて説明する。

【０１４８】ここで、プレーヤ１の端子４には、前記ディジタルコンテンツが記憶された記憶メディアが接続されているとする。

【０１４９】この状態で、ステップＳＴ１０１のように、当該プレーヤ１に対して、ユーザ端末５０から鑑賞を希望するディジタルコンテンツが指定される。このとき、当該指定は、例えばユーザ端末５０をユーザが操作することによりなされる。

【０１５０】このとき、プレーヤ１のコントローラ１６は、ステップＳＴ１０２のように、上記ユーザ端末５０からのコンテンツ指定情報に応じて、上記記憶メディアに対するアクセスを行い、コンテンツのＩＤを読み取る。

【０１５１】上記コントローラ１６は、ステップＳＴ１０３のように、上記記憶メディアから読み取ったコンテンツＩＤに基づき、前記共通鍵保管メモリ２２に対してアクセスを行い、コンテンツ鍵が格納されているかどうかを確認すると共に、前記ポイント使用情報格納メモリ２９に対してアクセスを行い、使用条件が格納されているかどうかを確認する。

【０１５２】ここで、上記共通鍵保管メモリ２２やポイント使用情報格納メモリ２９内に、上記コンテンツ鍵と使用条件が格納されていないことを確認したとき、コントローラ１６は、ユーザ端末５０に対して当該コンテンツ鍵等が存在しない旨の情報を送り、これによりユーザ端末５０からは上記コンテンツ鍵等の入手を促すメッセージを前記ディスプレイ装置に表示する。この場合は、前述したコンテンツ鍵入手用のフローチャートのようにしてコンテンツ鍵等を入手する。このように、新たにコンテンツ鍵等を入手した場合には、ステップＳＴ１０４にて前述したように、その暗号化されているコンテンツ鍵等を復号化する。

【０１５３】次に、コントローラ１６は、ステップＳＴ１０５に示すように、上記復号化された使用条件を元に、ポイント情報格納メモリ２８に格納されているポイント情報の残高が足りているかどうかを確認する。上記ポイント情報格納メモリ２８に格納された上記ポイント情報の残高が足りないときには、コントローラ１６からユーザ端末５０に対して当該ポイント情報の残高が足りない旨の情報が送られ、これによりユーザ端末５０は、上記ポイント情報の入手を促すメッセージを前記ディスプレイ装置に表示する。この場合、前述したようなポイント情報入手用のフローチャートのようにしてポイント情報を入手する。

【０１５４】ここで、実際にディジタルコンテンツの鑑賞を行うとき、コントローラ１６は、ステップＳＴ１０６のように、当該鑑賞するディジタルコンテンツに応じて上記ポイント情報格納メモリ２８からポイント情報数を減額し、さらに当該ポイント情報の使用状態に応じた新たなポイント使用情報を、ポイント使用情報格納メモリ２９に格納する（ポイント使用情報の更新を行う）。このようにポイント使用情報格納メモリ２９に対して新たに格納されるポイント使用情報としては、上記鑑賞したディジタルコンテンツに対応する権利者情報（著作権者等）と減額されたポイント情報数の情報その他の情報などである。

【０１５５】その後、コントローラ１６は、ステップＳＴ１０７のように、これらポイント情報の減額やポイント使用情報の新たな格納等の課金用処理が完了したことを確認すると、記憶メディアからディジタルコンテンツを読み出す。

【０１５６】この記憶メディアから読み出されたディジタルコンテンツは暗号化されているため、コントローラ１６は、ステップＳＴ１０９のように、上記暗号化されたディジタルコンテンツを共通暗号復号回路２４に転送する。

【０１５７】この共通暗号復号回路２４では、ステップＳＴ１１０のように、コントローラ１６からの指示に基づいて、先に復号化して共通鍵保管メモリ２２に保管されているコンテンツ鍵を用いて、上記暗号化されているディジタルコンテンツの復号化を行う。

【０１５８】また、このディジタルコンテンツは前述したように所定の圧縮処理がなされているため、コントローラ１６は、ステップＳＴ１１１のように、上記暗号が復号化された上記圧縮処理されているディジタルコンテンツを、上記共通暗号復号回路２４から伸長回路２６に転送させ、ここで上記所定の圧縮処理に対応する伸長処理を行わせる。

【０１５９】その後、当該伸長されたディジタルコンテンツは、ステップＳＴ１１２のように、Ｄ／Ａ変換回路２７にてアナログ信号に変換され、ステップＳＴ１１３のように、集積回路１０の端子１３と当該プレーヤ１のアナログ出力端子２とを介して外部（例えばユーザ端末５０等）に出力される。

【０１６０】以上により、コンテンツ鑑賞時のプレーヤ１における処理の流れが終了し、ユーザはディジタルコンテンツの鑑賞が可能となる。

【０１６１】次に、上述したようなディジタルコンテンツの鑑賞に伴って前記プレーヤ１のポイント使用情報格納メディア２９に新たに格納されたポイント使用情報を、管理センタ２１１に返却する際の、プレーヤ１、ユーザ端末５０、管センタ３１０における処理の流れについて、図２と図３を参照しながら、図２１から図２４を用いて説明する。

【０１６２】図２１には、ポイント使用情報返却時のプレーヤ１における処理の流れを示している。

【０１６３】この図２１において、コントローラ１６は、ステップＳＴ１２１に示すように、ユーザ端末５０

に予めインストールされているポイント使用情報返却用のソフトウェアの立ち上げが行われるまで待つ。

【０１６４】上記ユーザ端末５０の上記ポイント使用情報返却用のソフトウェアが立ち上がると、当該ソフトウェアに従ってユーザ端末５０に入力された情報が、ステップＳＴ１２２のように、前記ＰＣ用インターフェース端子３及び集積回路１０の端子１２を介して受信される。このときの上記ユーザ端末５０から供給される入力情報は、ユーザにより入力されるパスワード等である。

【０１６５】このコンテンツ指定情報を上記ユーザ端末５０から受信したコントローラ１６は、ステップＳＴ１２３にて、当該ユーザ端末５０から供給されたパスワードと、パスワード格納メモリ１４に格納されているパスワードとを比較して、当該パスワードが正しいどうかの確認をする。

【０１６６】上記パスワードの確認において正しいパスワードであると確認されたとき、コントローラ１６は、ステップＳＴ１２４のように、ポイント情報格納メモリ２８に格納されているポイント情報の残高と、ポイント使用情報格納メモリ２９に格納されているポイント使用情報とをそれぞれ読み出し、これら情報を暗号化する。

【０１６７】上記ポイント情報の残高とポイント使用情報の暗号化が終了すると、コントローラ１６は、ステップＳＴ１２５のように、ユーザＩＤ格納メモリ２３からユーザＩＤを読み出して上記暗号化したデータに添付する。

【０１６８】このユーザＩＤが添付されたデータは、ステップＳＴ１２６のように、コントローラ１６から端子１２及びＰＣ用インターフェース端子３を介してユーザ端末５０に転送される。このデータはその後管理センタ２１１に転送される。

【０１６９】なお、このときの暗号化にも前述したように共通鍵暗号方式が採用されている。すなわち、当該データの伝送に先立ち、前述同様に共通鍵の生成が行われ、この生成された共通鍵が前記公開鍵暗号方式にて暗号化（管理センタ２１１の公開鍵を用いた暗号化）され、ユーザＩＤと共に管理センタ２１１に送られている。

【０１７０】上述のようにしてユーザ端末５０にデータを転送した後、コントローラ１６は、上記管理センタ２１１から後述するデータがユーザ端末５０を介して転送されてくるのを待つ。

【０１７１】ここで、ステップＳＴ１２７のように上記管理センタ２１１からのデータを受信すると、プレーヤ１では、ステップＳＴ１２７のように、共通鍵暗号方式を使用して暗号化されている受信データを、前述同様に共通鍵を用いて復号化すると共にそのデータの正当性の確認を行う。すなわち、コントローラ１６は、上記復号化されたデータのセキュリティＩＤを、上記セキュリティＩＤ発生回路１９からのセキュリティＩＤとの比較によって確認することによる正当性の評価を行う。

【０１７２】また、上記管理センタ２１１から転送されてくるデータには、上記共通鍵を用いて暗号化された処理完了のメッセージも含まれている。したがって、上記セキュリティＩＤの確認が終了した後のコントローラ１６は、上記暗号化された処理完了メッセージを共通暗号復号回路２４に送り、ここで共通鍵を用いた復号化を行わせ、この復号化した処理完了メッセージを受け取ることで、上記管理センタ２１１での処理が完了したことを確認する。

【０１７３】以上により、ポイント使用情報返却時のプレーヤ１における処理の流れが終了する。

【０１７４】次に、ポイント使用情報返却時のユーザ端末５０における処理の流れを、図２２を用いて説明する。

【０１７５】この図２２において、ユーザ端末５０は、ステップＳＴ１３１にて、ポイント使用情報返却用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ１３２にて、上記ソフトウェアに従い当該ユーザ端末５０を操作するユーザに対して、パスワード等の入力要求を行い、ユーザからパスワードの入力がなされると、そのパスワードをプレーヤ１に転送する。

【０１７６】次に、ユーザ端末５０は、ステップＳＴ１３３にて、前記図２１のステップＳＴ１２６のように上記プレーヤ１にて作成されて転送されたデータを受信すると、ステップＳＴ１３４にて、当該プレーヤ１から転送されたデータを、予めアドレスが登録されている管理センタ２１１へ転送する。

【０１７７】上記管理センタ２１１に対してデータの転送を行った後のユーザ端末５０は、管理センタ２１１からの返送を待ち、ステップＳＴ１３５にて、管理センタ２１１からプレーヤ１に対して送られるデータを受信すると、当該データをそのままプレーヤ１に転送する。

【０１７８】上記プレーヤ１に対してデータの転送を行った後のユーザ端末５０は、処理が完了した旨をユーザに知らしめるための表示をディスプレイ装置に行い、ユーザからの確認を受ける。

【０１７９】以上により、ポイント使用情報返却時のユーザ端末５０における処理の流れが終了する。

【０１８０】次に、ポイント使用情報返却時の管理センタ２１１における処理の流れを、図２３を用いて説明する。

【０１８１】管理センタ２１１のユーザ端末との通信機能部１３３において、ステップＳＴ１４１のように、前記図２１のステップＳＴ１２６及び図２２のステップＳＴ１３４によって前記ユーザ端末５０を介してプレーヤ１から送信されてきたポイント使用情報等のデータを受信する。

【０１８２】このデータを受信すると、管理センタ２１

１のユーザ管理機能ブロック１１０は、ステップＳＴ１４２のように、コントロール機能部１１１の制御の元で、当該受信したデータに添付されたユーザＩＤに基づいて、データベース部１１２から前述同様に予め受け取って格納している共通鍵を入手すると共にセキュリティＩＤを入手する。

【０１８３】上記データベース部１１２から上記ユーザＩＤに対応する共通鍵とセキュリティＩＤを入手すると、ステップＳＴ１４３に示すように、管理センタ２１１のユーザ管理機能ブロック１１０の通信文暗号／復号機能部１１４において、上記共通鍵を用いて、上記プレーヤ１からの上記暗号化されたポイント使用情報等のデータの復号化を行い、さらにコントロール機能部１１１において、当該復号化したデータ中のセキュリティＩＤと上記データベース部１１２から読み出したセキュリティＩＤとの比較によって、アクセスしてきたユーザ側２００（プレーヤ１）が正当な使用者であるかどうかの内容確認を行う。

【０１８４】上記正当性と内容の確認後のデータは、使用情報管理機能ブロック１２０に転送される。この使用情報管理機能ブロック１２０のコントロール機能部１２１は、ステップＳＴ１４４に示すように、上記プレーヤ１から送られてきたポイント情報の残高とポイント使用情報とを用い、データベース部１２２に格納されている情報を用いて上記ユーザ側２００の使用に不正がないかどうかの確認を行う。同時に、当該不正なきことを確認した場合には、使用情報演算機能部１２３においてポイント情報の残高とポイント使用情報をまとめる演算を行う。

【０１８５】その後、ステップＳＴ１４５に示すように、ユーザ管理機能ブロック１１０のコントロール機能部１１１は、セキュリティＩＤ発生機能部１１６を制御してセキュリティＩＤを算出させ、さらに確認メッセージ発生機能部１１５を制御して処理完了のメッセージを生成させる。これらセキュリティＩＤと処理完了メッセージは、ユーザ管理機能ブロック１１０の通信文暗号／復号機能部１１４にて前記共通鍵を用いて暗号化される。

【０１８６】上記暗号化されて生成されたデータは、ステップＳＴ１４６に示すように、ユーザ端末との通信機能部１３３からユーザ端末５０に送られ、前記図２２のステップＳＴ１３５と図２１のステップＳＴ１２７のように当該ユーザ端末５０からプレーヤ１に転送されることになる。

【０１８７】以上により、ポイント使用情報返却時の管理センタ２１１における処理の流れが終了する。

【０１８８】上述した図２１から図２３の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図２４に示すように表すことができる。

【０１８９】すなわちこの図２４において、入力情報転送Ｔ３１では、前記図２２のステップＳＴ１３２のように、ユーザ端末５０からプレーヤ１に対して、前記パスワード等の入力情報が転送される。作成データ転送Ｔ３２では、前記図２１のステップＳＴ１２６のように、プレーヤ１が作成したデータがユーザ端末５０に転送される。作成データ転送Ｔ３３では、前記図２２のステップＳＴ１３４のように、上記プレーヤ１にて作成されたデータが上記ユーザ端末５０から管理センタ２１１に転送される。データ転送Ｔ３４では、前記図２３のステップＳＴ１４６のように、管理センタ２１１にて作成されたデータが、ユーザ端末５０に転送される。データ転送Ｔ３５では、前記図２１のステップＳＴ１２７のように、管理センタ２１１にて作成されたデータがユーザ端末５０を介してプレーヤ１に転送される。

【０１９０】本実施の形態のシステムのプレーヤ１とユーザ端末５０と管理センタ２１１の実際の動作は、上述したような流れとなる。

【０１９１】ここまでは、本実施の形態のシステムにおける全体の処理の流れを説明してきたが、これ以降は、本実施の形態のシステムの主要部の個々の動作を詳細に説明する。

【０１９２】先ず、本発明実施の形態における暗号化及び圧縮と、伸長及び復号化の動作についての説明を行う。

【０１９３】上述した実施の形態のシステムのように、ネットワークを使ってディジタルコンテンツを配信する際には、そのデータ量を抑えるために圧縮／伸長技術を使用し、コピー防止或いは課金のために暗号化／圧縮技術が使われる。すなわち、配信側（上述の例では管理センタ２１１側）でディジタルコンテンツを圧縮し、さらに暗号化処理することが行われる。上述の例のように送信側（管理センタ２１１側）にて生成されたディジタルコンテンツ（暗号化／圧縮データ）をネットワークを使って配信するとき、受信側（上述の例ではプレーヤ１）では上記暗号化及び圧縮されたディジタルコンテンツを受信後に復号化し、さらに伸長してディジタルコンテンツを復元することが行われる。なお、上記暗号化と圧縮、復号化と伸長の処理の順番は入れ替わる場合もある。

【０１９４】上記ディジタルコンテンツに著作権等が存在する場合、上記受信側は、上記ディジタルコンテンツを上記復号化と伸長する際に、上記著作権者等の意思に従い、課金されることになる。この課金は、主として復号化の鍵すなわちコンテンツ鍵を購入することにより行われるが、このコンテンツ鍵を購入する方法には種々ある。

【０１９５】ここで、上述したように、ディジタルコンテンツを圧縮して暗号化し、復号化して伸長するような処理手順に従った場合、例えば悪意を持ったユーザは上

記復号化済みの圧縮データを比較的簡単に入手することができることになる。すなわちディジタルコンテンツの圧縮データは、一般に容量が大きく、したがって例えば受信側の一般的なコンテンツ再生装置の内部メモリではなく、安価が外部メモリに蓄積される場合が多いため、この外部メモリから直接、或いは外部メモリとの接続部分で上記圧縮されたディジタルコンテンツを不正に取り出すことが容易だからである。

【０１９６】また、圧縮に対する伸長方式のアルゴリズムは公開されている場合が多く、また伸長方式のアルゴリズムには一般的な暗号の鍵のようにそれぞれ隠しておけば処理できないようなものも存在していない。しかも、上記復号化された圧縮ディジタルコンテンツは、上記送信側から配信された暗号化と圧縮とがなされたディジタルコンテンツと比較して、データ量的に変わらず、したがって、上記復号化された圧縮ディジタルコンテンツを悪意を持って配信するののも容易である。すなわち、上記圧縮した後に暗号化されてディジタルコンテンツを配信する方式によると、誰でも容易に伸長できる圧縮ディジタルコンテンツが、悪意を持ったユーザに容易に盗難され、このため著作権者等の意思の届かないところでさらに配信されたり、伸長されたりする危険性が大きい。

【０１９７】そこで、本発明の実施の形態では、このような状況に鑑み、ネットワークを使って配信するディジタルコンテンツの安全性を向上させることを可能にするため、上記図２のプレーヤ１において、以下の図２５のフローチャートに示すような処理を行っている。

【０１９８】すなわち図２のプレーヤ１の共通暗号復号回路２４における復号化処理と上記伸長回路２６における伸長処理では、前記記憶メディアから読み出された暗号化と圧縮処理されたディジタルコンテンツのデータを、ステップＳＴ１５１のように、先ず、復号化処理のアルゴリズムの処理単位Ｘビットと、伸長処理のアルゴリズム処理単位Ｙビットとの最小公倍数ｌｃｍ（Ｘ，Ｙ）の単位に分割する。

【０１９９】次に、上記最小公倍数ｌｃｍ（Ｘ，Ｙ）の単位に分割された上記暗号化と圧縮処理がなされているディジタルコンテンツのデータは、ステップＳＴ１５２に示すように、当該最小公倍数ｌｃｍ（Ｘ，Ｙ）の単位毎に、上記共通暗号復号回路２４にて復号化処理が行われる。

【０２００】当該復号化処理により得られた最小公倍数ｌｃｍ（Ｘ，Ｙ）の単位の圧縮されているディジタルコンテンツのデータは、ステップＳＴ１５４に示すように、当該単位分の全ての圧縮データに対して上記伸長回路２６にて伸長処理が行われる。

【０２０１】その後、この最小公倍数ｌｃｍ（Ｘ，Ｙ）の単位毎の復号化及び伸長処理は、上記暗号化と圧縮処理されたディジタルコンテンツの全データについての処理が終了するまで続けられる。すなわち、ステップＳＴ１５５に示すように、最小公倍数ｌｃｍ（Ｘ，Ｙ）の単位毎の復号化及び伸長処理がディジタルコンテンツの全データに対して完了したか否かの判断がなされ、完了していない時にはステップＳＴ１５２に戻り、完了したときに当該処理のフローチャートが終了する。

【０２０２】これにより全データの復号化及び伸長されたディジタルコンテンツが得られることになる。

【０２０３】なお、当該プレーヤ１における図２５のフローチャートの処理でも、上記最小公倍数ｌｃｍ（Ｘ，Ｙ）単位の復号化データは存在することになるが、当該復号化データのデータ量は少ない。このため、比較的高価でも安全性の高い内部メモリに保存することができるようになり、したがって前述したような外部メモリに保存する場合のように盗まれる可能性は非常に低いものとなる。

【０２０４】また、本実施の形態における上記プレーヤ１では、上記安全性を確保するための内部メモリとして、図２のバッファメモリ２５が上記共通暗号復号回路２４と伸長回路２６との間に設けられている。すなわちこのバッファメモリ２５は、１チップの集積回路１０内に設けられており、外部からアクセスされ難く、したがってデータが外部に取り出されることはない。

【０２０５】上述のフローチャートでは、最小公倍数ｌｃｍ（Ｘ，Ｙ）の単位分の全てのデータに対して復号化及び伸長処理を行うようにしており、このための具体的構成としては、例えば図２６に示す構成のように、最初に復号化処理のアルゴリズムの処理単位Ｘビットにディジタルコンテンツのデータを分割し、このＸビットのデータに復号化処理を施し、その後当該復号化処理されたＸビットの圧縮されているデータを、伸長処理のアルゴリズム処理単位Ｙビット分まとめ、当該Ｙビットの圧縮データを伸長することで、上述のように最小公倍数ｌｃｍ（Ｘ，Ｙ）の単位での復号化及び伸長処理を実現するようにしている。

【０２０６】このことを実現するプレーヤ１の共通暗号復号回路２４は、入力部３０と暗号復号部３１とからなり、上記伸長回路２６は、伸長部３２と出力部３３とからなる。これら共通暗号復号回路２４と伸長回路２６の間に前記バッファメモリ２５が設けられている。

【０２０７】ここで、より具体的な例として、上記ディジタルコンテンツに対する暗号化処理が例えばＤＥＳ（Data Encription Standard）暗号を用いて行われているのであれば、当該暗号化処理とそれに対応する復号化処理は、６４ビット単位で行われることになる。

【０２０８】また、圧縮されたディジタルコンテンツに対する伸長処理の場合、その圧縮率やサンプリング周波数によっても異なるが、現状では１Ｋ～２Ｋビット／チャンネル単位で処理される場合が多い。ここでは、便宜的に１．２８Ｋビット毎に処理されると仮定する。

【０２０９】したがって、上記ＤＥＳ暗号化方式と上記１．２８Ｋビット毎の圧縮伸長方式を用いたシステムの場合、上記最小公倍数ｌｃｍは１．２８Ｋとなる。

【０２１０】このような条件のもと、図２６の共通暗号復号回路２４の入力部３０には、前記暗号化されて圧縮されたディジタルコンテンツが入力される。当該入力部３１では、上記暗号化されて圧縮されたディジタルコンテンツを、上記復号化処理のアルゴリズムの処理単位Ｘビット、すなわち６４ビットづつのデータに分割して暗号復号部３１に出力する。

【０２１１】この暗号復号部３２では、上記Ｘビットすなわち６４ビットのデータを、当該６４ビット毎に復号化処理する。この６４ビット毎の復号化により得られた６４ビットの圧縮されているデータは、バッファメモリ２５に送られる。

【０２１２】当該バッファメモリ２５は、前記コントローラ１６からの指示に従い、伸長処理のアルゴリズム処理単位Ｙビット、すなわち１．２８Ｋビット分の圧縮データがたまった時点で、当該１．２８Ｋビット分の圧縮データを一括して出力し、この圧縮データが上記伸長回路２６の伸長部３２に送られる。

【０２１３】上記伸長部２６は、上記入力された１．２８Ｋビット分の圧縮データを伸長して出力部３３に出力する。

【０２１４】また、コントローラ１６は、バッファメモリ２５にたまったデータ量をモニタしながら、復号化部３１の処理と伸長部３２の処理をコントロールする。

【０２１５】なお、このケースであれば、復号化処理を２０個（＝１２８０／６４）並列で処理すれば、より高速な処理システムになる。

【０２１６】その他、前記図２や図２６のようなハードウェア構成ではなく、プログラマブルデバイスにて上述した処理を行う場合には、バッファメモリ２５の状況に応じて、例えばコントローラ１６が復号化プログラム或いは伸長プログラムに基づいて処理を行うことになる。

【０２１７】上述の説明では、圧縮した後に暗号化したディジタルコンテンツがプレーヤ１に供給され、プレーヤ１ではこの圧縮及び暗号化されたディジタルコンテンツを復号化した後に伸長する例を挙げたが、暗号化した後に圧縮されたディジタルコンテンツを伸長して復号化する場合であっても、上述同様の効果を得ることができる。

【０２１８】また、本発明は、圧縮／伸長並びに暗号化／復号化のアルゴリズムが限定されることはなく、いかなる方式に対しても有効である。

【０２１９】このように、本発明によれば、ネットワークを使って配信するディジタルコンテンツの安全性が向上する。

【０２２０】次に、前記セキュリティＩＤの発生動作についての説明を行う。

【０２２１】本実施の形態のように、ポイント情報を予め入手しておき、ディジタルコンテンツの鑑賞に応じて当該ポイント情報を減額するような方式の場合、前述したように、ネットワーク上の管理センタ２１１は、ユーザ側２００のユーザ端末５０からのポイント情報の購入依頼の通信を受けた後に、金融機関２２０その他と任意の確認を行った後、そのポイント情報を暗号化して、ユーザ側２００のプレーヤ１にネットワーク経由で送る。

【０２２２】本実施の形態のように、ポイント情報を予め入手しておき、ディジタルコンテンツの鑑賞に応じて当該ポイント情報を減額するような方式の場合、管理センタ２１１とプレーヤ１（ユーザ端末５０）との間で、ポイント情報の購入の度に、毎回同じようなデータのやり取りを行う（例えば暗号化された「３０００円分のポイント情報の補充要求」及びそれに対応した「３０００円分のポイント情報」といった情報のやりとりを行う）と、例えば悪意を持つ者による、金融機関２２０へのいわゆる「成り済まし」による金額補充が問題点となる。なお、ここに言う金融機関への「成り済まし」とは、上記悪意を持った者が本来のユーザ（本実施の形態ではユーザ側２００）に成り済まして、不正にポイント情報を入手するようなことを言う。

【０２２３】すなわち、ポイント情報の購入の度に毎回同じようなデータのやり取りを行っていると、例えば悪意を持った者が当該データを通信回線から盗み出して同じデータを生成し、管理センタ２１１に対して送り先を自分（悪意を持った者）にしてポイント情報の入手を依頼したような場合、当該悪意を持った者がポイント情報を入手できることになり、さらにこのポイント情報の購入代金の請求は本来のユーザ側２００になされることになるという問題が発生するおそれがある。

【０２２４】そこで、こういった不正を防止するために、本発明実施の形態のシステムでは、予め受信側（プレーヤ１側）と配信側（管理センタ２１１側）の両者で連動している乱数発生機能により発生させられた乱数を安全性向上のために使用している。本実施の形態では、上記乱数として前記セキュリティＩＤを発生している。なお、両者間で乱数発生を連動させるには、例えばユーザの登録手続きなどの際に、例えばタイマ１８を初期化するなどして、両者間の動作を同期させれば良い。

【０２２５】すなわち、この乱数（セキュリティＩＤ）を用いた場合の管理センタ２１１からプレーヤ１への例えばポイント情報入手時の動作は、以下のような流れとなる。

【０２２６】ポイント情報の購入時、管理センタ２１１からプレーヤ１に対して送られるデータは、前述したように例えばプレーヤ１から予め入手した共通鍵（セッション鍵）を用いて暗号化されたポイント情報と上記発生されたセキュリティＩＤからなるデータとなされる。

【０２２７】プレーヤ１のコントローラ１６は、当該管

理センタ２１１から受け取ったデータを前述したように共通暗号復号回路２４に送り、ここで前記共通鍵を用いて復号化処理を行う。これにより、管理センタ２１１から送られてきたポイント情報とセキュリティＩＤとが得られることになる。

【０２２８】その後、プレーヤ１のコントローラ１６は、上記管理センタ２１１から送られてきたセキュリティＩＤと、自身のセキュリティＩＤ発生回路１９にて発生したセキュリティＩＤとを比較する。この比較において、コントローラ１６は、管理センタ２１１からのセキュリティＩＤと、上記自身が発生したセキュリティＩＤとが一致したときのみ、上記管理センタ２１１から送られてきたポイント情報を、前記ポイント情報格納メモリ２８に格納する。

【０２２９】これにより、正当なユーザ側２００のプレーヤ１のみがポイント情報を入手できることになる。言い換えれば、正当なユーザ側２００のプレーヤ１と同じようなプレーヤを持っている悪意の者が、前記成り済ましによって不正にポイント情報を入手しようとしても、当該悪意の者が持っているプレーヤのセキュリティＩＤと上記管理センタ２１１から送られてきたセキュリティＩＤとは一致しないため、この悪意を持った者は前記成り済ましによる不正なポイント情報入手ができないことになる。

【０２３０】勿論、ユーザ側２００のプレーヤ１で発生するセキュリティＩＤは、当該プレーヤ１の集積回路１０内に設けられたセキュリティＩＤ発生回路１９によって発生されるものであり、外部には取り出せないものであるため、悪意を持った者が当該セキュリティＩＤを盗むことはできない。

【０２３１】上記セキュリティＩＤとしての乱数を発生する構成には種々のものがあるが、その一例を図２７に示す。この図２７の構成は、前記図２のセキュリティＩＤ発生回路１９の一具体例である。

【０２３２】この図２７において、一方向関数発生部４０は、いわゆる一方向性関数を発生する。なお、上記一方向性関数とは、比較的計算が簡単な関数で逆関数がはるかに計算が困難なものである。この一方向関数は、予め秘密通信等で受け取って当該一方向関数発生部４０に保存しておくことも可能である。なお、一方向関数発生部４０は、前記図２の集積回路１０内に設けられたタイマ１８からの時間情報を入力関数として上記一方向関数を発生するようにすることも可能である。上記一方向関数は、乱数決定部４３に送られる。

【０２３３】また、ユーザ定数発生部４１は、ユーザ毎に定められた所定のユーザ定数を発生する。このユーザ定数は、予め秘密通信等で送付されて当該ユーザ定数発生部４１に保存されるものである。なお、このユーザ定数は、例えば前記ユーザＩＤ格納メモリ２３が格納するユーザＩＤを用いることもできる。

【０２３４】乱数データベース４２は、乱数を格納するものであり、例えば９９個の乱数を格納している。

【０２３５】通信回数記憶部４４は、例えばコントローラ１６から送られてくる通信回数情報を記憶するものである。この通信回数情報とは、プレーヤ１と管理センタ２１１との間の通信回数を示す情報である。

【０２３６】これら一方向関数とユーザ定数と通信回数情報は、乱数決定部４３に送られる。当該乱数決定部４３は、例えば前記タイマ１８からの時間情報に基づき、上記一方向関数とユーザ定数から、予め乱数データベース部４２に記憶された範囲の乱数を発生させる（例えば９９個）。

【０２３７】すなわち、この乱数決定部４３では、上記通信回数情報が例えば１回目の通信であれば、９９個目の乱数を上記乱数データベース部４２から取り出し、また例えば通信回数情報がｎ回目の通信であれば１００－ｎ個目の乱数を上記乱数データベース４２から取り出し、この取り出した乱数を前記セキュリティＩＤとして出力する。

【０２３８】このセキュリティＩＤ発生の構成は、プレーヤ１と管理センタ２１１とで同じものを有している。

【０２３９】なお、乱数データベース部４２に格納している全ての乱数を使い終わったときには、上記乱数決定部４２において１００個～１９９個目の乱数を計算するか、或いは新たな乱数や１方向性関数を秘密通信するなどして、乱数データベース部４２に再格納したり、一方向性関数発生部４０に再構築する。

【０２４０】また、上述した説明では、乱数（セキュリティＩＤ）を発生させて通信毎の安全性を高めるようにしているが、本実施の形態では、前述のようにユーザ側２００と管理センタ２１１側との間で通信を行う毎に、毎回異なる共通鍵（セッション鍵）をプログラマブルに発生させるようにもしているので、さらに安全性が高められている。

【０２４１】ここで、実際に送信される送信文（例えばメッセージ等）について上記乱数が挿入されると共にセッション鍵による暗号化がなされる様子と、受信文から乱数が取り出されて正当性の確認がなされる様子を図２８と図２９を用いて説明する。なお、これら図２８、図２９の例では、送信文に署名（ディジタル署名）を付加するようにもしている。

【０２４２】この図２８において、先ず、前記共通鍵を公開鍵暗号方式にて暗号化して送信する流れとして、通信用共通鍵発生工程Ｐ７では前記セッション鍵を通信用に用いる共通鍵として発生し、この共通鍵は公開鍵暗号化工程Ｐ８にて受信側の公開鍵で暗号化される。この暗号化された共通鍵は、受信側に送られる。

【０２４３】一方、送信文としてのメッセージを共通鍵暗号方式にて暗号化して送信する場合の流れとして、例えばメッセージ生成行程Ｐ１ではメッセージＭが生成さ

れると共に、乱数発生工程Ｐ５にて乱数（前記セキュリティＩＤ）が発生される。これらメッセージＭと乱数は、共通鍵暗号化工程Ｐ６に送られる。この共通鍵暗号化工程Ｐ６では、上記通信用共通鍵発生工程Ｐ７にて発生した共通鍵を用いて、上記メッセージＭと乱数を暗号化する。

【０２４４】さらに、上記ディジタル署名を付加する場合、上記メッセージＭはハッシュ値計算工程Ｐ２に送られる。当該ハッシュ値計算工程Ｐ２では、上記メッセージＭからいわゆるハッシュ値が計算される。なお、ハッシュ値とはハッシュ法にて求められるアドレス情報であり、ハッシュ法とはデータ（この場合はメッセージＭ）の内容の一部（キーワード）に所定の演算を施し、その結果をアドレスとして使用するものである。このメッセージから生成されたハッシュ値（Ｍ）はディジタル署名として、秘密鍵暗号化工程Ｐ４に送られる。この秘密鍵暗号化工程Ｐ４では、送信側の秘密鍵で上記ディジタル署名を暗号化する。この暗号化されたディジタル署名は、共通鍵暗号化工程Ｐ６に送られる。これにより共通鍵暗号化工程Ｐ６では、上記通信用共通鍵発生工程Ｐ７にて発生した共通鍵を用いて、上記ディジタル署名を暗号化する。

【０２４５】これらメッセージＭとディジタル署名と乱数が受信側に送信される。

【０２４６】次に、図２９を用いて、図２８に対応する受信側での処理の流れを説明する。

【０２４７】この図２９において、先ず、前記共通鍵を公開鍵暗号方式にて復号化する流れとして、秘密鍵復号化工程Ｐ１１では、上記送信側から送信されてきた共通鍵を当該受信側の秘密鍵で復号化する。

【０２４８】一方、前記共通鍵暗号方式にて暗号化されたメッセージＭを復号化する流れとして、共通鍵復号工程１３では、上記送信されてきたメッセージＭを上記秘密鍵復号化工程Ｐ１１にて復号化した共通鍵を用いて復号化する。この復号化されたメッセージＭは、他機能送信工程Ｐ２０にて他の工程に送られることになる。

【０２４９】また、ディジタル署名を復号する流れでは、上記共通鍵復号化工程Ｐ１３にて復号化されたハッシュ値が、公開鍵復号化工程Ｐ１４にて送信側の公開鍵を用いて復号化される。同時に、ハッシュ値計算工程Ｐ１７では、上記メッセージＭからハッシュ値を計算する。これら公開鍵復号化工程Ｐ１４により復号化されたハッシュ値と上記ハッシュ値計算工程Ｐ１７にて計算されたハッシュ値とは、比較工程Ｐ１９にて比較され、改竄されていないことの確認が行われる。

【０２５０】さらに、送信された乱数については、上記共通鍵復号化工程Ｐ１３にて復号化された乱数と、当該受信側の乱数発生工程Ｐ２１にて発生された乱数とが、正当正確認工程Ｐ２２にて比較され、正当性の確認が行われる。

【０２５１】ところで、前述した図１に示した本実施の形態のシステムでは、ユーザ側２００に対するシステム側として、システム管理会社２１０と仮想店舗２３０とコンテンツプロバイダ２４０とが設けられている。なお、図１の金融機関２２０は、例えば外部の銀行等である。

【０２５２】上記システム管理会社２１０の管理センタ２１０は、仮想店舗２３０におけるディジタルコンテンツの展示や配信の管理、金融機関２２０との間でユーザ側２００の課金情報や各種情報の収集，分配及びそれらの管理、コンテンツプロバイダ２４０からのディジタルコンテンツの暗号化、扱う情報のセキュリティ管理など、システム側の主要な作業のほぼ全てを行っている。

【０２５３】しかし、上述したようなネットワークを使ってディジタルコンテンツを配信するシステムにおいて、ユーザ側がシステム側からディジタルコンテンツを入手する際や、ディジタルコンテンツの使用に伴う課金の際には、システム側に通信が集中することになり、ユーザ側に対して満足のいくレスポンスが得られなくなるおそれがある。

【０２５４】そこで、本発明の他の実施の形態では、システム管理会社２１０の機能、より具体的には管理センタ２１１の機能を、以下のように分割することで、上述したような通信の集中を防ぎ、通信のレスポンスを向上させることを可能にしている。

【０２５５】すなわち、本発明の他の実施の形態では、図３０に示すように、ユーザ側２００に対するシステム側の構成を、ディジタルコンテンツを展示，配信する機能を有するコンテンツ展示配信機関３１０と、一定の地域のユーザの課金情報を管理する機能を有する課金情報管理機関３２０と、ディジタルコンテンツを暗号化する等のデータ生成と上記コンテンツ展示配信機関３１０への生成データの配信と上記課金情報管理機関３２０からの情報収集と収益分配とシステム全体のセキュリティ管理その他を行う機能を有するシステム管理機関３３０とに分割し、各機関３１０，３２０，３３０がそれぞれ独立にユーザ側２００と通信可能になされている。

【０２５６】この図３０のような構成において、コンテンツ展示配信機関３１０は、世界中のネットワーク上に散らばって複数配置可能なものであり、ユーザ側２００は通信費さえ支払えばどの地域のコンテンツ展示配信機関３１０へでもアクセスできる。例えばユーザ側２００がディジタルコンテンツを入手したい場合には、ユーザ側２００から上記コンテンツ展示配信機関３１０にアクセスして、ディジタルコンテンツを入手する。このときのディジタルコンテンツは、システム管理機関３３０によって暗号化等されたディジタルコンテンツ、すなわちユーザ側２００にネットワークを使って直接送信可能な状態になされたものである。

【０２５７】また、課金情報管理機関３２０は、課金情

報を扱うため、余り多くのユーザを抱え込むことは安全性管理上好ましくなく、したがって、適度な数のユーザ毎に設置する。但し、あまり多く設置すると、悪意を持った第３者からの攻撃ポイント（課金情報管理機関３２０）を増やすことになり、トレードオフになるので、最適化することが望ましい。例えばユーザ側２００が課金に関する通信を行う場合には、ユーザ側２００から上記課金情報管理機関３２０に対してアクセスする。

【０２５８】上記システム管理機関３３０は、ユーザのシステムへの加入や決済方法の登録、ユーザからの集金や前記権利者，コンテンツ展示配信機関３１０，課金情報管理機関３２０等の利益受益者への利益配付など、セキュリティ上重要な情報の管理をまとめて行うことで、セキュリティを向上させる。但し、当該システム管理機関３３０は世界に１箇所のみ設けるわけではなく、あるまとまった単位、例えば国などの単位で設置するのが望ましい。例えば、ユーザ側２００がこのシステムへの加入や決済方法の登録などセキュリティ上重要な通信を行う場合には、ユーザ側２００から上記システム管理機関３３０に対してアクセスして行う。当該ユーザからの集金と利益受益者への利益配付は上記課金情報管理機関３２０から情報を入手した当該システム管理機関３３０がまとめて行う。また、著作権者等が有するソースデータすなわちコンテンツは、当該システム管理機関３３０に供給され、ここで暗号化等がなされたディジタルコンテンツに変換され、上記コンテンツ展示配信機関３１０に配信される。

【０２５９】上述のように、システム側の機能を例えば３つの機関３１０，３２０，３３０に振り分け、ユーザ側２００と各機関３１０，３２０，３３０との間で直接アクセス可能とすることにより、通信の集中を防ぎ、通信のレスポンスを向上させることが可能となる。また、コンテンツ展示配信機関３１０によれば、既存のいわゆるバーチャルモールのようなものにも対応でき、販売促進にも有効であり、ユーザにとって魅力のあるものになる。課金情報管理機関３２０を別に分けることにより、コンテンツの展示や販売機能と結託した不正防止に役立つ。また、管理するユーザを一定の数に抑えられるため、不正に対する管理機能もより効果的である。

【０２６０】以下に、上述した図３０に示した本発明の他の実施の形態のシステムにおいて、ユーザのシステムへの加入、ポイント情報の購入や暗号化されたディジタルコンテンツの復号用のコンテンツ鍵等の入手時の情報の流れ、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れ、コンテンツの使用に伴う課金情報の流れについて説明する。

【０２６１】先ず、図３１を用いて、ユーザのシステムへの加入時の流れの主要部を説明する。

【０２６２】ユーザのシステムへの加入登録の際には、システム管理機関３３０のユーザ加入サポート機能ブロック４０２による以下の手順の従って登録作業が行われる。

【０２６３】ユーザ側２００すなわち前記プレーヤ１及びユーザ端末５０からは、先ず加入意思送付Ｔ４１のように、システムへの加入の意思を示す情報が、システム管理機関３３０に対してネットワークを介して送付される。システム管理機関３３０の通信機能ブロック４０１に入力された上記加入意思の情報は、ユーザ加入サポート機能ブロック４０２に送られる。

【０２６４】当該ユーザ加入サポート機能ブロック４０２は、上記加入意思情報を受信すると、加入必要ファイル送付Ｔ４２のように、加入に必要なファイルの情報を通信機能ブロック４０１を介してユーザ側２００に送られる。

【０２６５】ユーザ側２００では、上記システム管理機関３３０から送られてきた加入必要ファイルに基づいて、所定のフォーマットに従った加入申請書の作成が行われる。当該作成された加入申請書は、加入申請書送付Ｔ４３のように、システム管理機関３３０に送付される。

【０２６６】上記加入申請書を受け取ったユーザ加入サポート機能ブロック４０２は、クライアント機能送付Ｔ４４のように、クライアントの機能を解説する情報を、ユーザ側２００に送付する。

【０２６７】当該クライアント機能の情報を受け取ったユーザ側２００からは、ユーザ情報送付Ｔ４５のように、ユーザ側の情報、例えば前述したような口座番号やクレジット番号，名前や連絡先等のユーザ情報を、システム管理機関３３０に送付する。

【０２６８】当該ユーザ情報の送付を受けたユーザ加入サポート機能ブロック４０２は、登録手続き完了通知Ｔ４６のように、加入の登録手続きが完了した旨の情報を、ユーザ側２００に通知する。

【０２６９】また、このユーザ加入登録の手続き完了後、システム管理機関３３０のユーザ加入サポート機能ブロック４０２は、ユーザ情報送付Ｔ４７のように、通信機能ブロック４０１を介して、課金情報管理機関３２０に対してユーザ情報を転送する。このユーザ情報を受け取った課金情報管理機関３２０は、当該ユーザ情報をデータベース機能ブロック３６７に保存する。

【０２７０】以上により、ユーザのシステムへの加入時の主な流れが終了する。なお、この図３１に挙げられている他の構成についての説明は後述する。

【０２７１】次に、図３２を用いて、ポイント情報の購入や暗号化されたディジタルコンテンツの復号用の鍵等の入手時の情報の流れの主要部を説明する。なお、上記ポイント情報の購入や暗号化されたディジタルコンテンツの復号用のコンテンツ鍵の情報は、コンテンツを使用するための情報であるので、以下の説明では、これらを簡略化して使用権情報と呼ぶことにする。

【０２７２】ユーザがシステムで使用する重要な情報（ここでは、コンテンツの使用権）を入手する際は、予めユーザ側２００毎に担当割当がなされている課金情報管理機関３２０に対し、ユーザ側２００からアクセスがなされる。上記ユーザ側２００から送られてくるコンテンツ使用権情報の入手要求のアクセスに対しては、課金情報管理機関３２０の使用権発行機能ブロック３６２が対応し、以下の手順に従って使用権の発行が行われる。

【０２７３】先ず、ユーザ側２００からは、購入依頼書送付Ｔ５１のように、使用権を購入したい旨の情報が課金情報管理機関３２０に対して送付される。使用権を購入したい旨の情報は、ユーザ側２００によって所定のフォーマットに従った購入依頼書の情報である。このようにネットワークを介し、この課金情報管理機関３２０の通信機能ブロック３６１に入力された上記購入依頼書の情報は、使用権発行機能ブロック３６２に送られる。

【０２７４】当該使用権発行機能ブロック３６２では、上記購入依頼書の情報を受け取ると、データベース機能ブロック３６７に保存されたユーザ情報を元にして、新しい使用権の情報を生成し、新規使用権送付Ｔ５２のように、当該使用権の情報をユーザ側２００に対して送付する。

【０２７５】ユーザ側２００は、上記新規使用権の情報の受取を確認すると、所定のフォーマットに従った受取確認書を作成し、受取確認書送付Ｔ５３のように、課金情報管理機関３２０の使用権発行機能ブロック３６２に送付する。

【０２７６】以上により、使用権の購入時の主な流れが終了する。なお、この図３２に挙げられている他の構成についての説明は後述する。

【０２７７】次に、図３３を用いて、コンテンツとコンテンツ鑑賞用の情報（ここでは使用条件とコンテンツ鍵）の流通の際の流れの主要部を説明する。

【０２７８】先ず、コンテンツ展示配信機関３１０のコンテンツ入手機能ブロック３４２は、コンテンツ請求書送付Ｔ６２のように、システム管理機関３３０に対して、ディジタルコンテンツを請求する。

【０２７９】当該コンテンツ請求書を受け取ったシステム管理機関３３０は、コンテンツ配布機能ブロック４０４において、要求されたコンテンツを流通できるように加工する。すなわち、このコンテンツ配布機能ブロック４０４では、ユーザ側２００に送付可能な状態のディジタルコンテンツ（暗号化されたディジタルコンテンツ）を生成する。この加工されたディジタルコンテンツは、コンテンツ送付６３のように、コンテンツ展示配信機関３１０に送られる。

【０２８０】当該コンテンツ展示配信機関３１０では、上記加工されたディジタルコンテンツを、コンテンツデータベース機能ブロック３４５に保存する。

【０２８１】また、システム管理機関３３０のコンテンツ配布機能ブロック４０４では、コンテンツ鑑賞用の情報として、コンテンツＩＤと使用条件と暗号化されたコンテンツを復号するためのコンテンツ鍵とを、コンテンツ鑑賞用情報送付Ｔ６４のように、課金情報管理機関３２０に送付する。

【０２８２】課金情報管理機関３２０では、上記コンテンツ鑑賞用の情報を、コンテンツ鍵・使用条件受取機能ブロック３６３にて受理し、データベース機能ブロック３６７に保存する。

【０２８３】次に、ユーザ側２００は、コンテンツ入手依頼Ｔ６１のように、コンテンツ展示配信機関３１０に対してアクセスし、コンテンツを入手する。すなわち、コンテンツ展示配信機関３１０は、通信機能ブロック３４１を介して上記ユーザ側２００からコンテンツの入手の要求がなされると、コンテンツデータベース機能ブロック３５４に保存している暗号化されたディジタルコンテンツを読み出し、当該読み出したディジタルコンテンツをユーザ側２００の送付する。

【０２８４】その後、ユーザ側２００は、コンテンツ鑑賞用情報請求Ｔ６５にて課金情報管理機関３２０に対してアクセスし、コンテンツ鑑賞用情報送付Ｔ６６のようにコンテンツ鑑賞用の情報を入手する。すなわち、課金情報管理機関３２０では、通信機能ブロック３６１を介して、上記ユーザ側２００からコンテンツ鑑賞用の情報として使用条件とコンテンツ鍵の請求がなされると、コンテンツ鍵・使用条件発行機能ブロック３６４からコンテンツ鍵と使用条件とを発行し、これらを通信機能ブロック３６１を介してユーザ側２００に送付する。

【０２８５】以上により、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れが終了する。なお、この図３３に挙げられている他の構成についての説明は後述する。

【０２８６】次に、図３４を用いて、コンテンツが実際に鑑賞されたときの精算、すなわちコンテンツ使用料金の精算の流れの主要部を説明する。

【０２８７】先ず、ユーザ側２００にてコンテンツの鑑賞が行われた後、当該ユーザ側２００からは、精算書送付Ｔ７１のように、例えば前述のようにしてポイント使用情報すなわちコンテンツの使用記録が課金情報管理機関３２０に対して送付される。このように通信機能ブロック３６１を介して上記ユーザ側２００から上記コンテンツ使用記録の送付を受けると、課金情報管理機関３２０の精算手続き受付機能ブロック３６５にて当該コンテンツ使用記録を受け取り、これに対応する精算確認書を発行する。当該精算確認書は、精算確認書送付Ｔ７３のように、同じく通信機能ブロック３６１を介してユーザ側２００に送付される。これにより、ユーザ側２００は精算が行われたことを知ることができる。

【０２８８】次に、課金情報管理機関３２０の精算手続き受付機能ブロック３６５は、使用権発行機能ブロック

３６２から使用権発行情報を発行させる。この使用権発行情報は、上記ユーザ側２００から送られてきたコンテンツ使用記録と共に、通信機能ブロック３６１を介し、ユーザ決済・コンテンツ使用記録送付Ｔ７４としてシステム管理機関３３０に送付される。

【０２８９】システム管理機関３３０は、集金及び分配機能ブロック４０５にて、各地に分散している課金情報管理機関３２０から送付されてきた情報をまとめ、集金額と集金先とお金の分配先を集計し、実際の金融機関を通して決済する。

【０２９０】以上により、コンテンツ使用料金の精算の流れが終了する。なお、この図３４に挙げられている他の構成についての説明は後述する。

【０２９１】上述の図３０から図３４までの説明において、コンテンツ展示配信機関３１０、課金情報管理機関３２０、システム管理機関３３０とユーザ側２００との間のデータ送受や、コンテンツ展示配信機関３１０、課金情報管理機関３２０とシステム管理機関３３０との間のデータ送受においても、前述同様にデータの暗号化と復号化が行われていることは言うまでもない。またこの暗号化と復号化においても、公開鍵暗号方式と共通鍵暗号方式の何れを用いても良いし、前述したようにコンテンツ鍵や共通鍵の暗号化方式としては公開鍵暗号方式を使用し、メッセージや各種の書類等の暗号化方式としては共通鍵暗号方式を使用することができる。また、これら暗号化と共に前記乱数を用いたセキュリティ向上の手法や、コンテンツを扱う際の暗号化と圧縮の処理単位の最小公倍数化を使用することも可能である。

【０２９２】次に、上述した各機関３１０、３２０、３３０の具体的な構成について簡単に説明する。

【０２９３】先ず、図３５を用いてコンテンツ展示配信機関３１０の構成の説明を行う。

【０２９４】この図３５において、当該コンテンツ展示配信機関３１０は、大別して、ユーザ側２００とシステム管理機関３３０との間の通信機能を担当する通信機能ブロック３４１と、コンテンツの入手機能を担当するコンテンツ入手機能ブロック３４２と、コンテンツの展示機能を担当するコンテンツ展示機能ブロック３４３と、精算を担当する精算機能ブロック３４４と、コンテンツを保存するコンテンツデータベース機能ブロック３４５とからなる。

【０２９５】上記コンテンツ入手機能ブロック３４２は、システム管理機関３３０に対してコンテンツを請求するときの請求書の作成を担当するコンテンツ請求書作成機能部３５１と、システム管理機関３３０からコンテンツを受け取ったときの受領書の作成を担当するコンテンツ受領書作成機能部３５２と、これらあつかったコンテンツとコンテンツデータベース機能ブロック３４５に保存しているコンテンツとの対応を担当するコンテンツデータベース対応機能部３５３とからなる。

【０２９６】上記コンテンツ展示機能ブロック３４３は、実際に仮想店舗にコンテンツを展示する機能を担当するコンテンツ展示機能部３５４と、これら展示しているコンテンツと上記コンテンツデータベース機能ブロック３４５に保存しているコンテンツとの対応を担当するコンテンツデータベース対応機能部３５５とからなる。

【０２９７】上記精算機能ブロック３４４は、領収書を発行する機能を担当する領収書発行機能部３５６と、金融機関２２０との間の対応を担当する金融機関対応機能部３５７とからなる。

【０２９８】次に、図３６を用いて、課金情報管理機関３２０の構成の説明を行う。

【０２９９】この図３６において、当該課金情報管理機関３２０は、大別して、ユーザ側２００とシステム管理機関３３０との間の通信機能を担当する通信機能ブロック３６１と、使用権を発行する機能を担当する使用権発行機能ブロック３６２と、コンテンツ鍵と使用条件の受け取りを担当するコンテンツ鍵・使用条件受取機能ブロック３６３と、コンテンツ鍵と使用条件の発行を担当するコンテンツ鍵・使用条件発行機能ブロック３６４と、精算手続きの受け付け機能を担当する精算手続き受付機能ブロック３６５と、分配と受け取りの機能を担当する分配受取機能ブロック３６６と、データベース機能ブロック３７６とからなる。

【０３００】上記使用権発行機能ブロック３６２は、購入依頼書の確認機能を担当する購入依頼書確認機能部３７１と、クライアントすなわちユーザ側２００の使用権の残高（ポイント情報の残高）や使用記録（ポイント使用情報）等のデータの確認を担当するポイントデータ確認機能部３７２と、使用権を発生する機能を担当する使用権発生機能部３７３と、使用権の送付書を作成する機能を担当する使用権送付書作成機能部３７４と、使用権と使用権送付書を実際に送付する機能を担当する送付機能部３７５と、使用権の受け取り書の確認を担当する使用権受取確認機能部３７６と、発行した使用権の情報を保存する機能を担当する使用権発行情報保存機能部３７７とからなる。

【０３０１】上記コンテンツ鍵・使用条件受取機能ブロック３６３は、コンテンツ鍵と使用条件の受取を担当する受取機能部３７８と、コンテンツ鍵と使用条件を保存する保存機能部３７９とからなる。

【０３０２】上記コンテンツ鍵・使用条件発行機能ブロック３６４は、コンテンツ鍵と使用条件の入手依頼を受信する機能を担当する受信機能部３８０と、コンテンツ鍵と使用条件をデータベース機能ブロック３６７から検索して探し出す機能を担当する検索機能部３８１と、コンテンツ鍵と使用条件を暗号化して送付する機能を担当する送信機能部３８２と、コンテンツ鍵と使用条件の受取書の確認機能を担当する確認機能部３８３とからなる。

【０３０３】上記精算手続き受付機能ブロック３６５は、暗号化されているコンテンツ使用記録（ポイント使用情報）を受信して復号化する機能を担当するコンテンツ使用記録受信機能部３８４と、コンテンツ使用記録の確認を担当するコンテンツ使用記録確認機能部３８５と、コンテンツ使用記録をデータベース機能ブロック３６７の保存する機能を担当するコンテンツ使用記録保存機能部３８６と、精算手続きの完了書を作成する機能を担当する完了書作成機能部３８７と、コンテンツ使用記録をまとめて編集する機能を担当するまとめ機能部３８９とからなる。

【０３０４】上記分配受取機能ブロック３６６は、集金を行う際の資料を請求する資料請求書の確認機能を担当する請求書確認機能部３９０と、システム管理機関３３０に対して提出するコンテンツ使用記録の報告書を作成する機能を担当する使用記録報告書作成機能部３９１と、システム管理機関３３０に対して提出する使用権発行情報の報告書を作成する機能を担当する使用権発行報告書作成機能部３９２と、報告書の受信確認書の確認機能を担当する確認書確認機能部３９３とからなる。

【０３０５】データベース機能ブロック３６７は、使用権のデータを保存する機能を担当する使用権データベース機能部３９４と、コンテンツ鍵と使用条件のデータを保存する機能を担当するコンテンツ鍵・使用権データベース機能部３９５と、コンテンツ使用記録を保存するコンテンツ使用記録データベース機能部３９６と、ユーザに関する情報を保存するユーザ管理データベース機能部３９７とからなる。

【０３０６】次に、図３７を用いて、システム管理機関３３０の構成の説明を行う。

【０３０７】この図３７において、当該システム管理機関３３０は、大別して、ユーザ側２００、コンテンツ展示配信機関３１０、及び課金情報管理機関３２０との間の通信機能を担当する通信機能ブロック４０１と、ユーザ加入の際のサポートを行うユーザ加入サポート機能ブロック４０２と、コンテンツの配布を担当するコンテンツ配布機能ブロック４０４と、データベース機能ブロック４０３と、集金と分配の機能を担当する集金及ぶ分配機能ブロック４０５とからなる。

【０３０８】上記ユーザ加入サポート機能ブロック４０２は、加入申請書の作成と送信を担当する加入申請書作成送信機能部４１１と、暗号化された共通鍵を受信して復号化する機能を担当する共通鍵受信機能部４１２と、ユーザ側２００から送信されてきた加入申請書の確認機能を担当する加入申請書確認機能部４１３と、クライアントＩＤすなわちユーザＩＤを発生する機能を担当するＩＤ発生機能部４１４と、加入申請書をデータベース機能ブロック４０３に保存する機能を担当する加入申請書保存機能部４１５と、クライアント機能を生成するクライアント機能生成機能部４１６と、登録情報をデータベース機能ブロック４０３に保存する機能を担当する登録情報保存機能部４１７とからなる。

【０３０９】データベース機能ブロック４０３は、ユーザの情報を保存管理するユーザ管理データベース機能部４１８と、コンテンツを保存するコンテンツデータベース機能部４１９と、課金情報管理機関３２０の情報を保存管理する課金情報管理機関データベース機能部４２０と、コンテンツ展示配信機関３１０の情報を保存管理するコンテンツ展示配信機関データベース機能部４２１とからなる。

【０３１０】コンテンツ配信機能ブロック４０４は、コンテンツの請求書の確認機能を担当する請求書確認機能部４２２と、生コンテンツすなわち加工前のコンテンツ（ソースデータ）をデータベース機能ブロック４０３のコンテンツデータベース機能部４１９から検索する機能を担当するコンテンツ検索機能部４２３と、コンテンツＩＤを生成するコンテンツＩＤ生成機能部４２４と、コンテンツ鍵を生成するコンテンツ鍵生成機能部４２５と、コンテンツ使用条件を生成するコンテンツ使用条件生成機能部４２６と、生コンテンツすなわち加工前のコンテンツを圧縮するコンテンツ圧縮機能部４２７と、コンテンツの暗号化を行うコンテンツ加工機能部４２８と、コンテンツＩＤとコンテンツ鍵と使用条件とをデータベース機能ブロック４０３のコンテンツデータベース機能部４１９に保存する機能を担当する保存機能部４２９と、コンテンツを通信機能ブロック４０１を介して送付する機能を担当するコンテンツ送付機能部４３０と、コンテンツの受領書を確認する機能を担当するコンテンツ受領書確認機能部４３１と、コンテンツＩＤとコンテンツ鍵と使用条件を通信機能ブロック４０１を介して送付する機能を担当するＩＤ・鍵・使用条件送付機能部４３２と、コンテンツＩＤとコンテンツ鍵と使用条件の受領書を確認する機能を担当するＩＤ・鍵・使用条件受領書確認機能部４３３とからなる。

【０３１１】集金及び分配機能ブロック４０５は、集金に使用する資料の請求書を作成する資料請求書作成機能部４３４と、コンテンツ使用権を通信機能ブロック４０１を介して受信する機能を担当するコンテンツ使用権受信機能部４３５と、コンテンツ使用記録を通信機能ブロック４０１を介して受信する機能を担当するコンテンツ使用記録受信機能部４３６と、受信の確認書を作成する機能を担当する受信確認書作成機能部４３７と、ユーザへ請求する請求額の計算と請求書の作成を行う請求書の作成を行う計算・請求書作成機能部４３８と、使用により集金した使用金を権利者に分配する際の分配金の計算と納付書の作成を行う計算・納付書作成機能部４３９とからなる。

【０３１２】次に、当該他の実施の形態のシステムに対応するユーザ側２００の構成を、図３８を用いて説明する。なお、この図３８は、前記プレーヤ１とユーザ端末

５０の各機能をまとめて表している。

【０３１３】この図３８において、当該ユーザ側２００の構成は、大別すると、システム管理機関３３０、コンテンツ展示配信機関３１０、及び課金情報管理機関３２０との間の通信機能を担当する通信機能ブロック４５１と、コンテンツの入手を担当するコンテンツ入手機能ブロック４５２と、ポイント情報やコンテンツ鍵、使用条件等の使用権の購入を担当する使用権購入機能ブロック４５３と、コンテンツ鍵と使用条件の入手を担当するコンテンツ鍵・使用条件入手機能ブロック４５４と、精算手続きを担当する精算手続き機能ブロック４５５と、システムへの加入をサポートする機能を担当するユーザ加入サポート機能ブロック４５６と、コンテンツの鑑賞と課金の機能を担当するコンテンツ鑑賞課金機能ブロック４５７と、データベース機能ブロック４５８とからなる。

【０３１４】上記コンテンツ入手機能ブロック４５２は、実際にコンテンツを入手する機能を担当するコンテンツ入手機能部４６１と、コンテンツを記憶メディアに保存させる機能を担当するコンテンツ保存機能部４６２とからなる。

【０３１５】使用権購入機能ブロック４５３は、使用権の購入依頼書を作成する購入依頼書作成機能部４６３と、クライアント（ユーザ）の使用権の残高（ポイント残高）や使用記録（ポイント使用情報）等のデータのまとめを担当するまとめ機能部４６４と、使用権としての各情報をインストールする機能を担当する使用権インストール機能部４６５と、使用権受取書を作成する使用権受取書作成機能部４６７とからなる。

【０３１６】コンテンツ鍵・使用条件入手機能ブロック４５４は、コンテンツ鍵と使用条件の入手依頼書を作成する入手依頼書作成機能部４６８と、コンテンツ鍵と使用条件の受信を担当する受信機能部４６９と、コンテンツ鍵と使用条件の受取書を作成する受取書作成機能部４７０とからなる。

【０３１７】精算手続き機能ブロック４５５は、コンテンツ使用記録（ポイント使用情報）のまとめを行うまとめ機能部４７１と、精算手続きの完了書の受信を担当する完了書受信機能部４７２とからなる。

【０３１８】上記ユーザ加入サポート機能ブロック４５６は、加入申請書の作成を担当する加入申請書作成機能部４７３と、クライアント機能のインストールすなわちユーザのプレーヤ１の初期化を担当するクライアント機能インストール機能部４７４、登録情報を作成する機能を担当する登録情報作成機能部４７５とからなる。

【０３１９】コンテンツ鑑賞課金機能ブロック４５７は、記憶メディアに保存されたコンテンツの検索を担当するコンテンツ検索機能部４７６と、使用権の確認を担当する使用権確認機能部４７７と、例えばコンテンツの選択を行うときに簡易的にコンテンツを再生する簡易コンテンツ鑑賞機能部４７８と、課金情報（ポイント情報）の管理を行う課金機能部４７９と、暗号化されているコンテンツを復号化するコンテンツ復号機能部４８０と、圧縮されているコンテンツを伸長するコンテンツ伸長機能部４８１と、例えば記憶メディアに保存されているコンテンツの内容を認識可能にするためのコンテンツビューア機能部４８２とからなる。

【０３２０】データベース機能ブロック４５８は、使用権のデータを保存する使用権データベース機能部４８３と、コンテンツ鍵と使用条件を保存するコンテンツ鍵・使用条件データベース機能部４８４と、コンテンツ使用記録を保存するコンテンツ使用記録データベース機能部４８５と、ユーザ情報を保存するユーザ情報データベース機能部４８６とからなる。

【０３２１】次に、上述したような各実施の形態のプレーヤ１とユーザ端末５０の具体的な使用形態について、図３９と図４０を用いて説明する。

【０３２２】図３９に示すように、プレーヤ１は、前記アナログ出力端子２とＰＣ用インターフェース端子３と記憶メディア用Ｉ／Ｏ端子４がプレーヤ１の筐体外に突き出た状態で配置されており、上記記憶メディア用Ｉ／Ｏ端子４には、記憶メディア６１が接続されるようになっている。また、これらプレーヤ１と記憶メディア６１は、例えばケース６０内に収納可能に形成されており、このケース６０の例えば一端側に上記プレーヤ１のアナログ出力端子２とＰＣ用インターフェース端子３が配置されるようになされている。

【０３２３】このプレーヤ１及び記憶メディア６１が収納されたケース６０は、上記プレーヤ１のアナログ出力端子２とＰＣ用インターフェース端子３が配置される側から、上記ユーザ端末５０としてのパーソナルコンピュータ５０の入出力ポート５３に挿入接続可能なように形成されている。

【０３２４】当該パーソナルコンピュータ５０は、コンピュータ本体に、ディスプレイ装置５２とキーボード５４とマウス５５とを備えた一般的な構成を有するものであるが、上記入出力ポート５３内には上記プレーヤ１のアナログ出力端子２及びＰＣ用インターフェース端子３と対応したインターフェースが形成されている。したがって、上記プレーヤ１及び記憶メディア６１が収納されたケース６０を上記パーソナルコンピュータ５０の入出力ポート５３に挿入するだけで、上記プレーヤ１のアナログ出力端子２とＰＣ用インターフェース端子３が上記パーソナルコンピュータ５０と接続されるようになる。

【０３２５】上記図３９の例では、パーソナルコンピュータ５０の入出力ポート５３内に、上記プレーヤ１のアナログ出力端子２及びＰＣ用インターフェース端子３と対応したインターフェースを形成するようにしているが、例えば図４０に示すように、パーソナルコンピュータ５０の汎用入出力ポートのインターフェースに対応で

きるアダプタ６２を、上記プレーヤ１のアナログ出力端子２及びＰＣ用インターフェース端子３の間に配置することも可能である。

【０３２６】以上述べてきたことから、本発明の実施の形態のシステムにおいては、ディジタルコンテンツはシステムの共通鍵であるコンテンツ鍵にて暗号化されているので、本実施の形態のシステムに登録したユーザ（プレーヤ１）であれば、この暗号化されたコンテンツを自由にコピーでき、コンテンツ鍵を入手しさえすればこのコンテンツの鑑賞も可能である。したがって、このコンテンツ（暗号化されたコンテンツの）記憶メディアへのインストールも簡単に行える。一方、本実施の形態システムに準拠していない端末装置では、暗号化されたディジタルコンテンツを復号できないので、コンテンツの著作権や当該コンテンツの権利者の権利は保護される。

【０３２７】また、本発明の実施の形態システムによれば、ポイント情報をプリペイド方式（料金前払い方式）により補充することにし、コンテンツ鑑賞時にポイント情報が減額されるようにするとともに、そのポイントの使用情報を収集するようにしているので、使用済みのポイントに関する権利をもつ権利者（著作権者等）及びコンテンツ販売店舗等は、鑑賞代金の回収が可能である。

【０３２８】さらに、ポイント情報やポイント使用情報のデータのやりとりの際には、前述したように暗号化が施されているので、セキュリティ性が向上している。例えば全く前回のデータと同じものを偽造して課金用のポイント情報を盗もうとしても、前述したように、システム側とプレーヤ側とで連動した乱数（セキュリティＩＤ）を使用し、両者が一致していることを確認してから取引を行うものとしているので、安全である。

【０３２９】またさらに、プレーヤの主要構成要素は１チップ化されており、鍵情報や復号化されたディジタルコンテンツを外部に取り出すことが困難となっている。このプレーヤ１は、当該プレーヤ１の破壊によるデータ横取りを防ぐためにプレーヤ１自体にタンパーレジスタンス機能を備えている。

【０３３０】上述したように、本発明の実施の形態によれば、セキュリティ上強度の高いディジタルコンテンツ配信システムが構築されている。

【０３３１】なお、上述のディジタルコンテンツとしては、ディジタルオーディオデータの他に、ディジタルビデオデータ等の各種のものを挙げることができる。上記ディジタルビデオデータとして動画像データ（オーディオデータも含む）使用した場合、前記圧縮の手法としては、例えばＭＰＥＧ（Moving Picture Image CodingExperts Group）等の圧縮手法を使用できる。なお、上記ＭＰＥＧは、ＩＳＯ（国際標準化機構）とＩＥＣ（国際電気標準会議）のＪＴＣ（Joint Technical Committee）１のＳＣ（Sub Committee）２９のＷＧ（Working Group）１１においてまとめられた動画像符号化方式の通称であり、ＭＰＥＧ１，ＭＰＥＧ２，ＭＰＥＧ４等がある。

【０３３２】さらに、上記暗号化の手法としては、前述したように、例えばいわゆるＤＥＳ（Data Encryption Standard）と呼ばれている暗号化手法を使用することができる。なお、ＤＥＳとは、米国のＮＩＳＴ（National Institute of Standards and Technology）が１９７６年に発表した標準暗号方式（暗号アルゴリズム）である。具体的には、６４ビットのデータブロック毎にデータ変換を行うものであり、関数を使った変換を１６回繰り返す。上記ディジタルコンテンツやポイント情報等は、当該ＤＥＳを用い、いわゆる共通鍵方式にて暗号化されている。なお、上記共通鍵方式とは、暗号化するための鍵データ（暗号鍵データ）と復号化するための鍵（復号鍵データ）が同一となる方式である。

【０３３３】また、前記図１のプレーヤ１の共通鍵保管メモリ２２や通信用鍵保管メモリ２１、ポイント使用情報格納メモリ２９、ポイント情報格納メモリ２８等には、例えばいわゆるＥＥＰＲＯＭ（電気的に消去可能なＲＯＭ）を使用できる。

【０３３４】他に記憶メディアとしては、例えばハードディスクやフロッピィディスク、光磁気ディスク，相変化型光ディスク等の記録媒体、或いは半導体メモリ（ＩＣカード等）の記憶メディアを使用できる。

【０３３５】その他、上述の実施の形態では、コンテンツの選択や仮想店舗２３０に展示されたコンテンツの内容確認等の際には、ユーザ端末５０のキーボード５４やマウス５５、ディスプレイ装置５２を使用して選択、確認等を行っていたが、これらキーボードやマウス、ディスプレイ装置に機能を簡略化して、プレーヤ１に持たせることも可能である。すなわち。図２のように、入力キー部６や表示部７をプレーヤ１に設けることも可能である。

【０３３６】

【発明の効果】以上の説明で明らかなように、本発明によれば、簡単に持ち運びができて何時でも何処でもディジタルコンテンツを楽しむことが可能であり、また、ディジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築することをも可能である。

【図面の簡単な説明】

【図１】本発明の実施の形態のディジタルコンテンツ配布システムの全体構成を示すシステム構成図である。

【図２】本発明の実施の形態のシステムに対応するプレーヤの具体的構成を示すブロック回路図である。

【図３】本発明の実施の形態のシステムに対応する管理センタの具体的構成を示すブロック回路図である。

【図４】本実施の形態のシステムにおいてプレーヤの購入時の手順の説明に用いる図である。

【図５】本実施の形態のシステムにおいてディジタルコ

ンテンツの検索からプレーヤ用の記憶メディアへのディジタルコンテンツのインストールまでの手順の説明に用いる図である。
【図６】実施の形態のシステムにおいて課金用のポイント情報の購入と当該ディジタルコンテンツを使用した場合の精算の手順の説明に用いる図である。
【図７】実施の形態のシステムにおいて課金代金の分配の手順の説明に用いる図である。
【図８】実施の形態のシステムにおいてポイント購入時のプレーヤにおける処理の流れを示すフローチャートである。
【図９】実施の形態のシステムにおいてポイント購入時のユーザ端末における処理の流れを示すフローチャートである。
【図１０】実施の形態のシステムにおいてポイント購入時の管理センタにおける処理の流れを示すフローチャートである。
【図１１】実施の形態のシステムにおいてポイント購入時の情報送受のシーケンスを示す図である。
【図１２】実施の形態のシステムにおいてディジタルコンテンツの入手時のプレーヤにおける処理の流れを示すフローチャートである。
【図１３】実施の形態のシステムにおいてディジタルコンテンツの入手時のユーザ端末における処理の流れを示すフローチャートである。
【図１４】実施の形態のシステムにおいてディジタルコンテンツの入手時の管理センタにおける処理の流れを示すフローチャートである。
【図１５】実施の形態のシステムにおいてディジタルコンテンツの入手時の情報送受のシーケンスを示す図である。
【図１６】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時のプレーヤにおける処理の流れを示すフローチャートである。
【図１７】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時のユーザ端末における処理の流れを示すフローチャートである。
【図１８】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時の管理センタにおける処理の流れを示すフローチャートである。
【図１９】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時の情報送受のシーケンスを示す図である。
【図２０】実施の形態のシステムにおいてプレーヤとユーザ端末を用いてディジタルコンテンツを実際に鑑賞する際の処理の流れを示すフローチャートである。
【図２１】実施の形態のシステムにおいてポイント使用情報返却時のプレーヤにおける処理の流れを示すフローチャートである。
【図２２】実施の形態のシステムにおいてポイント使用情報返却時のユーザ端末における処理の流れを示すフローチャートである。
【図２３】実施の形態のシステムにおいてポイント使用情報返却時の管理センタにおける処理の流れを示すフローチャートである。
【図２４】実施の形態のシステムにおいてポイント使用情報返却時の情報送受のシーケンスを示す図である。
【図２５】暗号化と圧縮の処理単位の最小公倍数にて復号化と伸長を行う際の処理の流れを示すフローチャートである。
【図２６】暗号化と圧縮の処理単位の最小公倍数の単位毎の復号化及び伸長処理を行う構成を示すブロック回路図である。
【図２７】セキュリティＩＤとしての乱数を発生する具体的構成を示すブロック回路図である。
【図２８】共通鍵を公開鍵暗号方式にて暗号化して送信する際に乱数が挿入される様子を説明するための図である。
【図２９】受信文から乱数が取り出されて正当性の確認がなされる様子を説明するための図である。
【図３０】システム側の機能を分割したときの各機関の説明に用いる図である。
【図３１】システム側の機能を分割した実施の形態において、ユーザのシステムへの加入時の流れの主要部を説明するための図である。
【図３２】システム側の機能を分割した実施の形態において、ポイント情報の購入や暗号化されたディジタルコンテンツの復号用の鍵等の入手時の情報の流れの主要部を説明するための図である。
【図３３】システム側の機能を分割した実施の形態において、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れの主要部を説明するための図である。
【図３４】システム側の機能を分割した実施の形態において、コンテンツが実際に鑑賞されたときの精算の流れの主要部を説明するための図である。
【図３５】システム側の機能を分割した実施の形態において、コンテンツ展示配信機関の構成を示すブロック図である。
【図３６】システム側の機能を分割した実施の形態において、課金情報管理機関の構成を示すブロック図である。
【図３７】システム側の機能を分割した実施の形態において、システム管理機関の構成を示すブロック図である。
【図３８】システム側の機能を分割した実施の形態において、ユーザ側の構成を示すブロック図である。
【図３９】プレーヤとユーザ端末の具体的な使用形態の一例の説明に用いる図である。
【図４０】プレーヤとユーザ端末の具体的な使用形態の他の例の説明に用いる図である。

【図４１】従来の圧縮／伸長技術を使用してコピー防止或いは課金を行う構成の一例であり、圧縮後に暗号化を行う構成を示すブロック回路図である。

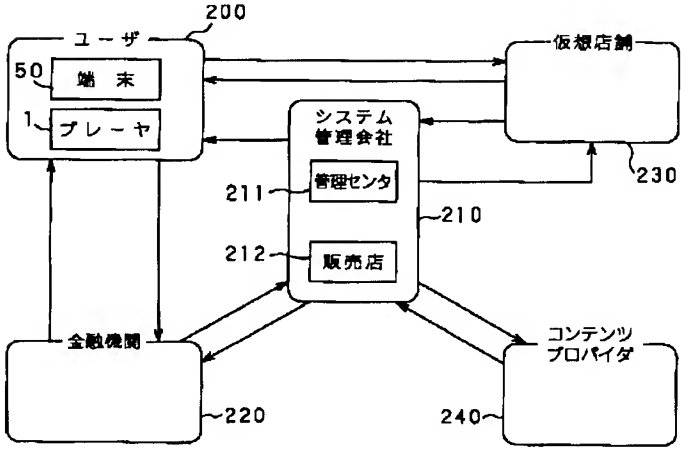
【図４２】圧縮後に暗号化が行われたデータを受信側で復号化及び伸長処理する際の流れを示すフローチャートである。

【図４３】従来の圧縮／伸長技術を使用してコピー防止或いは課金を行う構成の一例であり、暗号化後に圧縮を行う構成を示すブロック回路図である。

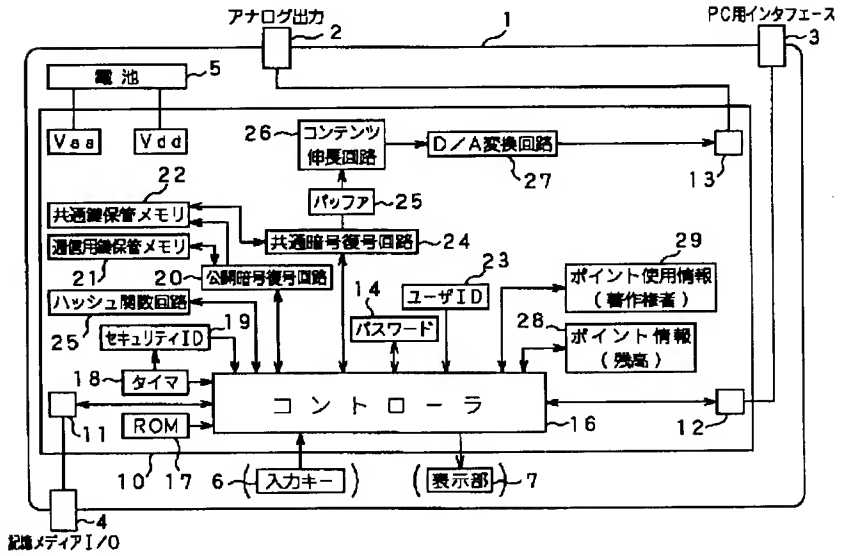
【符号の説明】

１　プレーヤ、　２　アナログ出力端子、　３　ＰＣ用インターフェース端子、　４　記憶メディア用Ｉ／Ｏ端子、　１６　コントローラ、　１９　セキュリティＩＤ発生回路、　２０　公開暗号復号回路、　２１　通信用鍵保管メモリ、２２　共通鍵保管メモリ、　２３　ユーザＩＤ格納メモリ、　２４　共通暗号復号回路、　２５　バッファメモリ、　２６　伸長回路、　２７　Ｄ／Ａ変換回路、　５０　ユーザ端末、　１００　コンテンツ管理機能ブロック、　１１０ユーザ管理機能ブロック、　１２０　使用情報管理機能ブロック、　１３０　管理機能ブロック、　２００　ユーザ側、　２１０　システム管理会社、　２１１管理センタ、　２２０　金融機関、　２３０　仮想店舗、　２４０　コンテンツプロバイダ

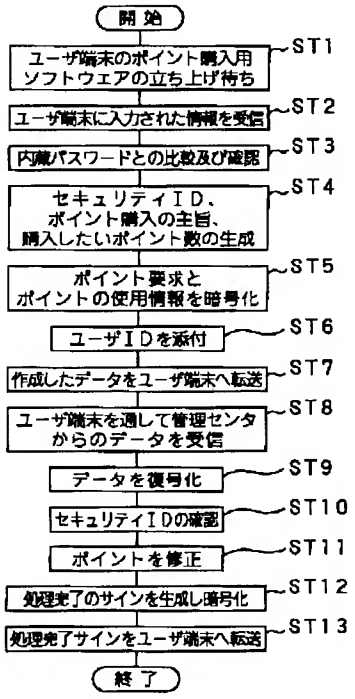
【図１】



【図２】

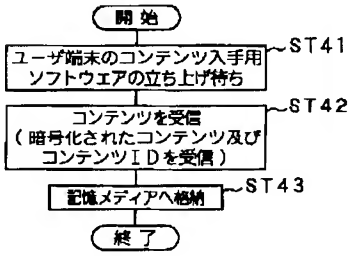


【図８】



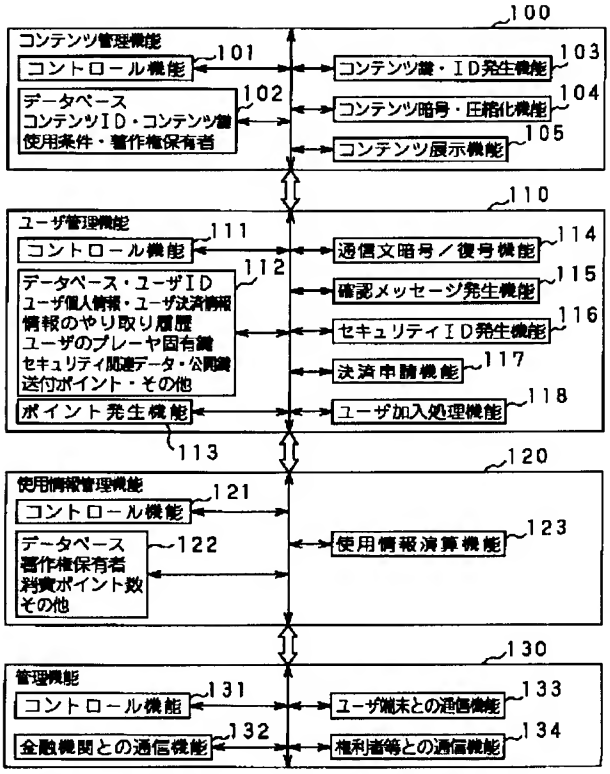
ポイント購入時のプレーヤのフローチャート

【図１２】

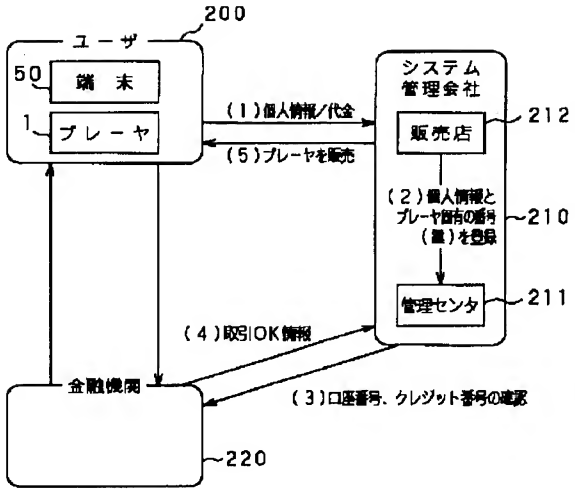


コンテンツ入手時のプレーヤのフローチャート

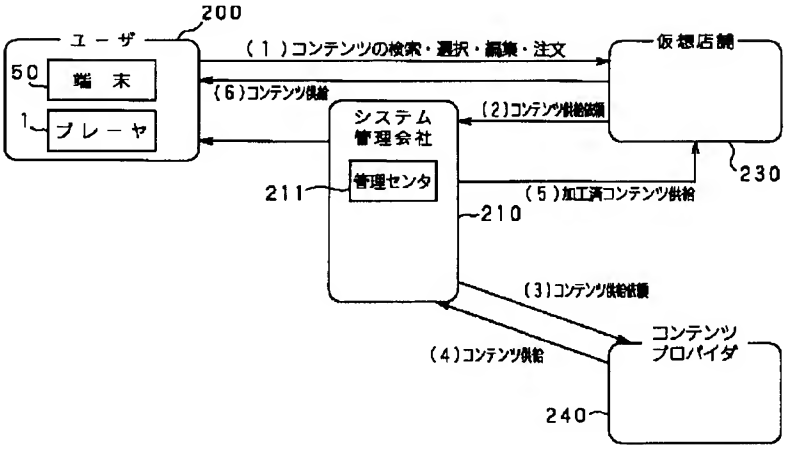
【図３】



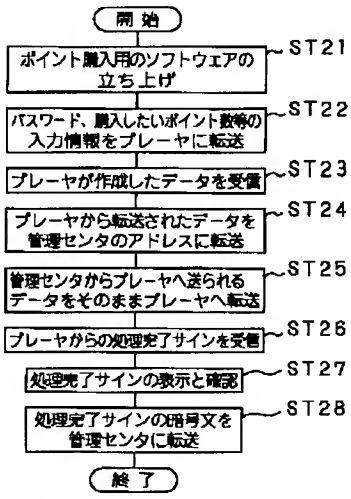
【図４】



【図５】

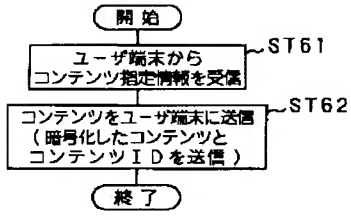


【図９】



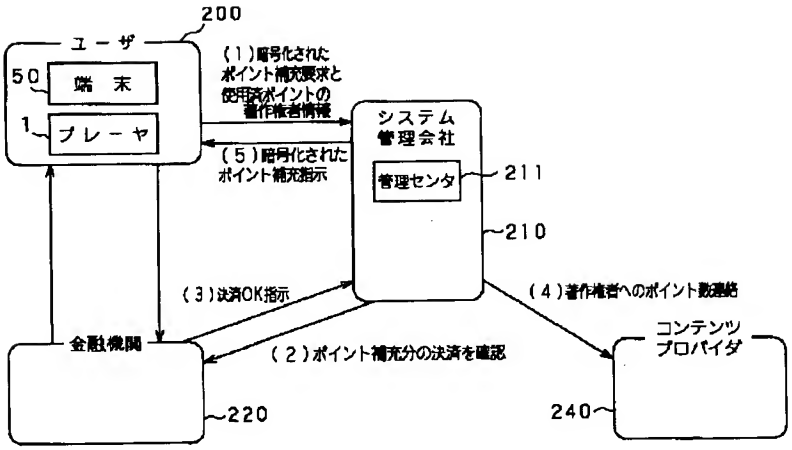
ポイント購入時のユーザ端末のフローチャート

【図１４】

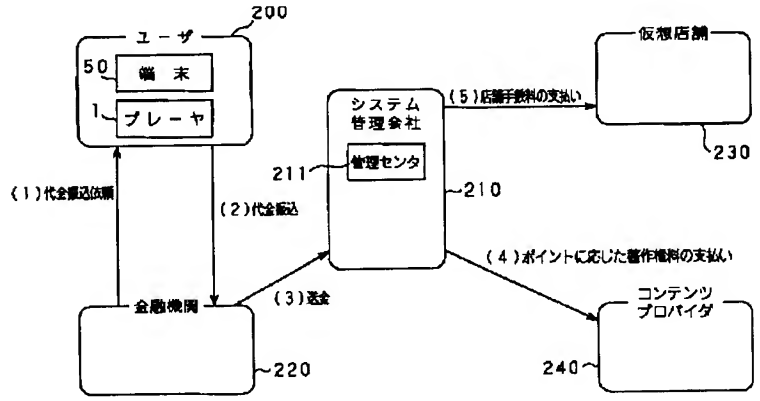


コンテンツ入手時の管理センタのフローチャート

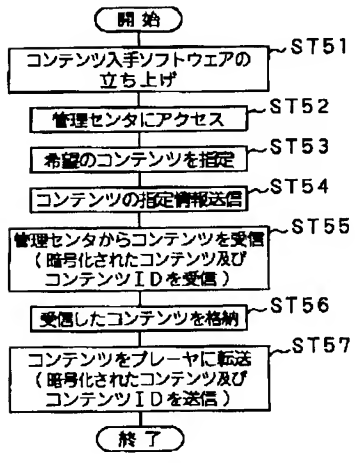
【図６】



【図７】

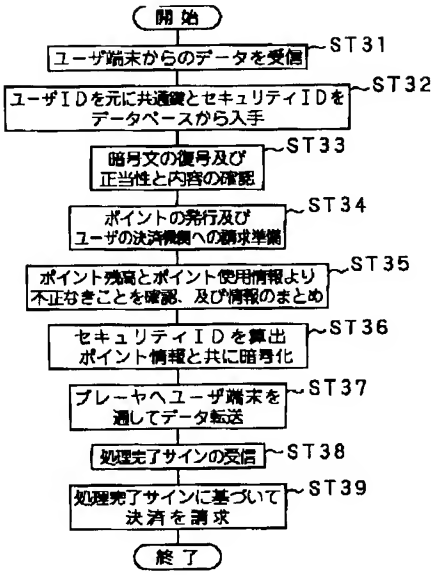


【図１３】



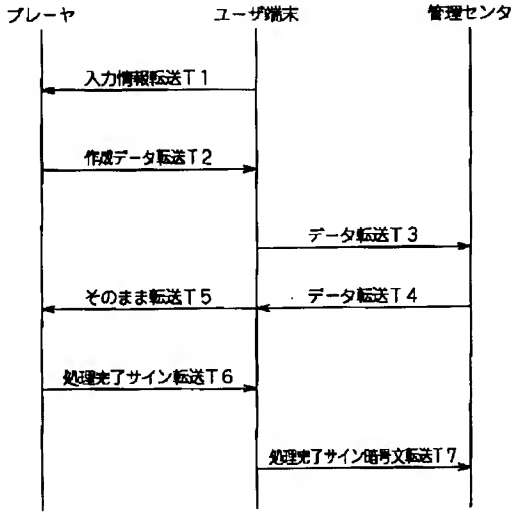
コンテンツ入手時のユーザ端末のフローチャート

【図１０】



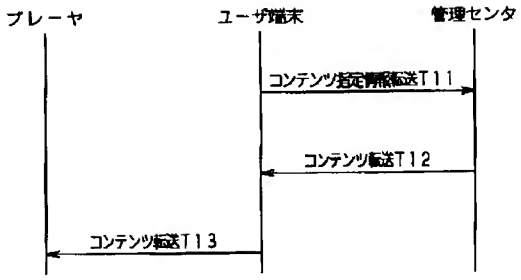
ポイント購入時の管理センタのフローチャート

【図１１】



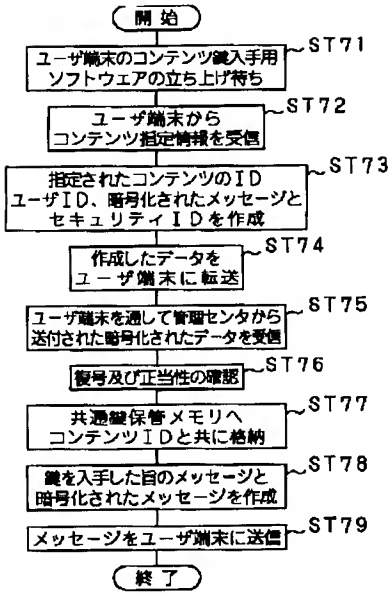
ポイント購入時のシーケンス

【図１５】



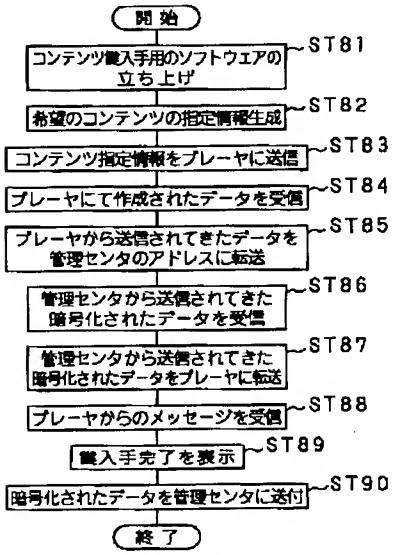
コンテンツ入手時のシーケンス

【図１６】



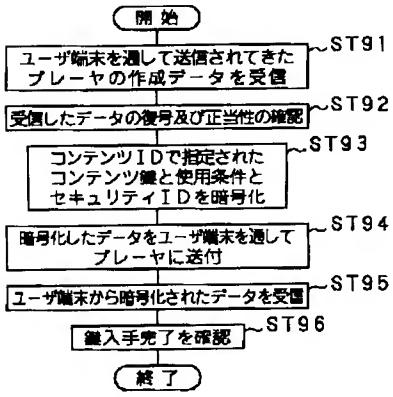
コンテンツ鍵・入手時のプレーヤのフローチャート

【図１７】



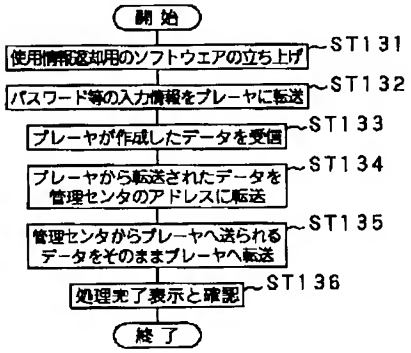
コンテンツ鍵・使用条件入手時のユーザ端末のフローチャート

【図１８】



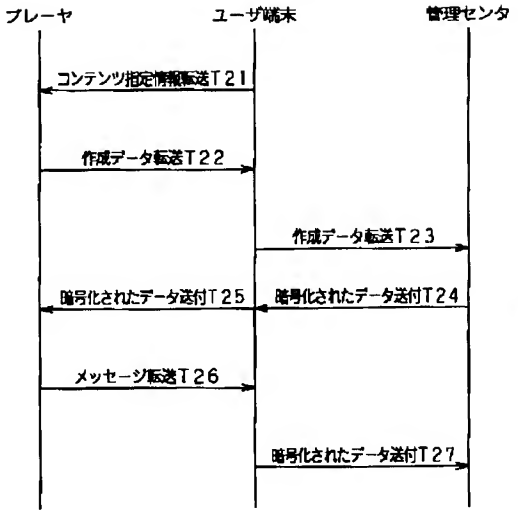
コンテンツ鍵・使用条件入手時の管理センタのフローチャート

【図２２】



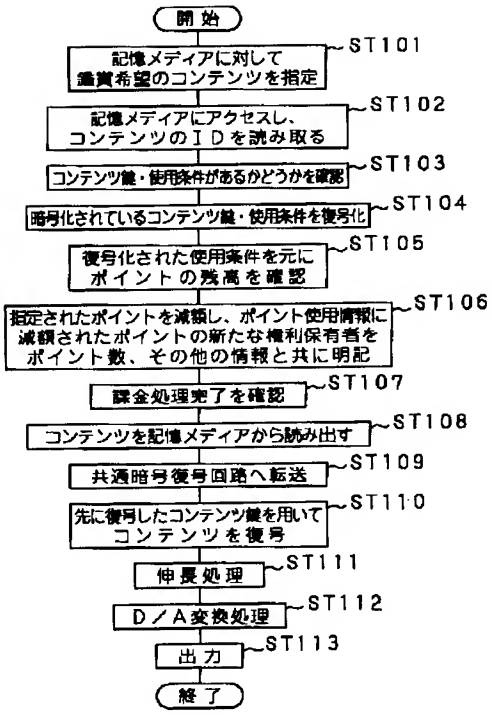
使用情報返却時のユーザ端末のフローチャート

【図１９】



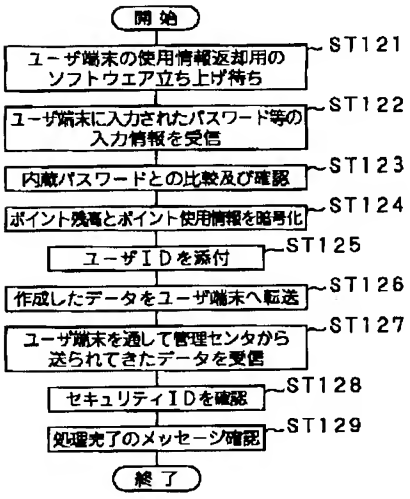
コンテンツ鍵・使用条件入手時のシーケンス

【図２０】



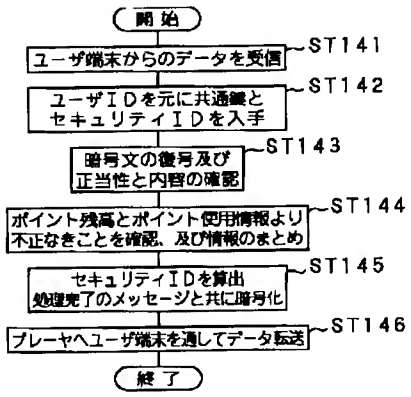
コンテンツ重資時のプレーヤのフローチャート

【図２１】



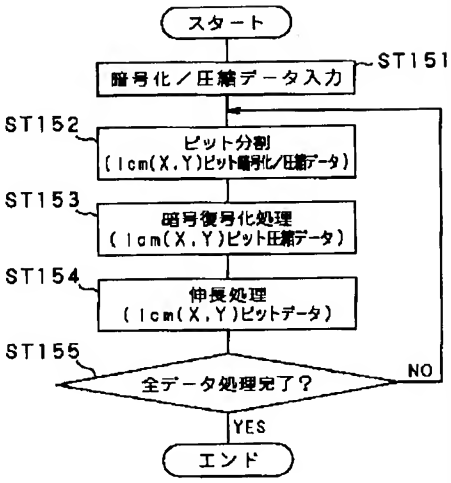
使用情報返却時のプレーヤのフローチャート

【図２３】

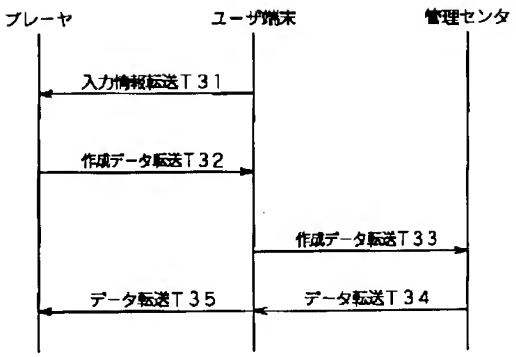


使用情報返却時の管理センタのフローチャート

【図２５】

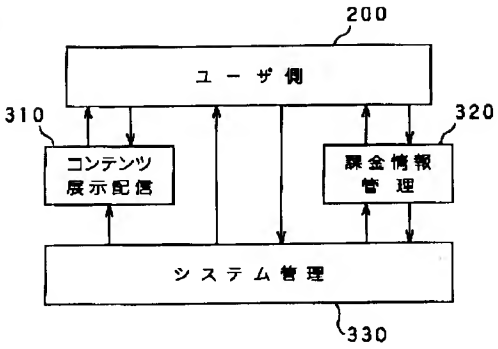


【図２４】

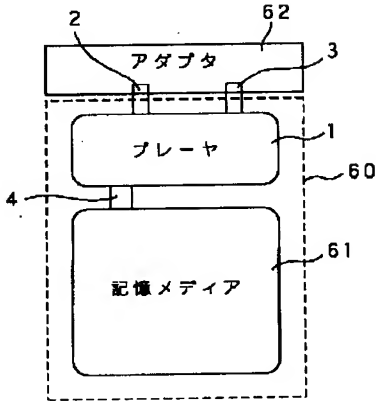


使用情報返却時のシーケンス

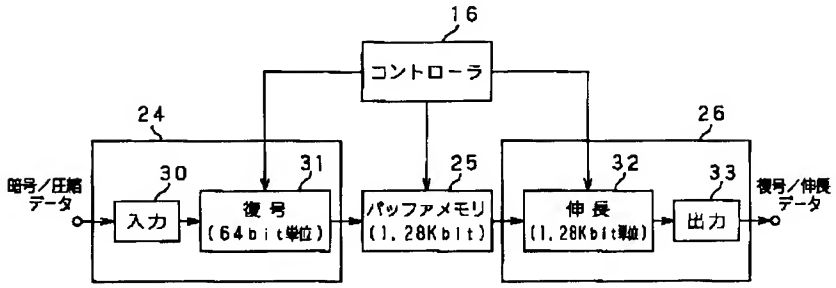
【図３０】



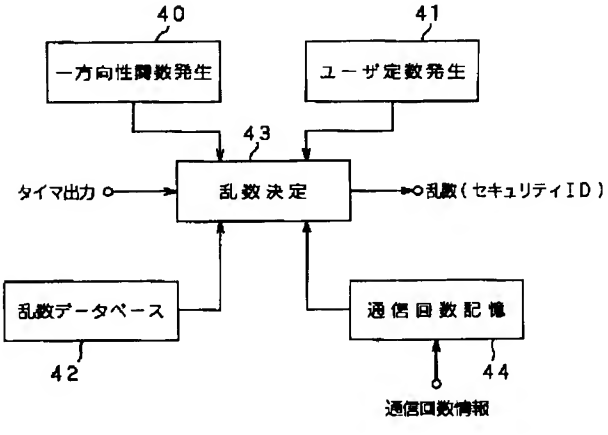
【図４０】



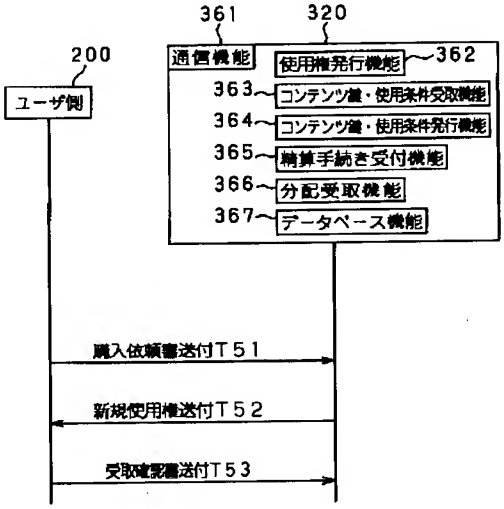
【図２６】



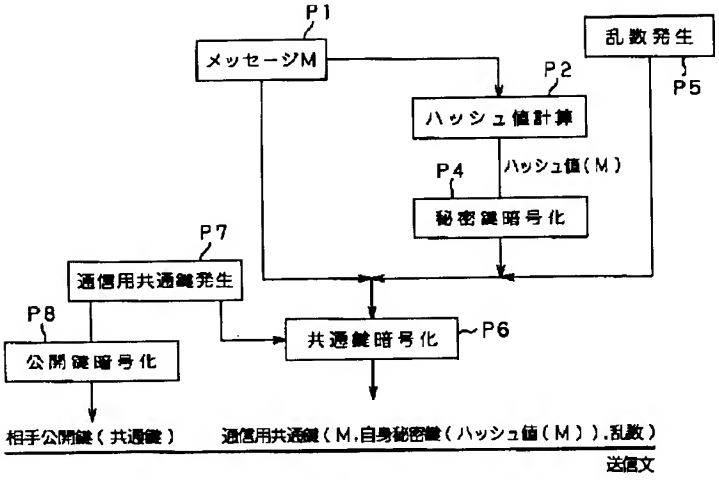
【図２７】



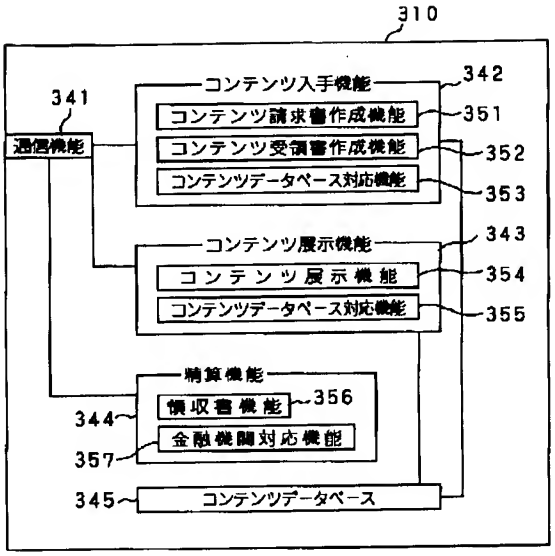
【図３２】



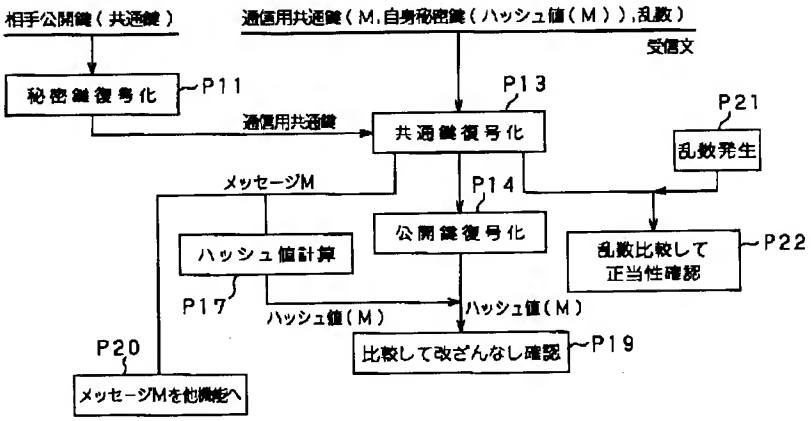
【図２８】



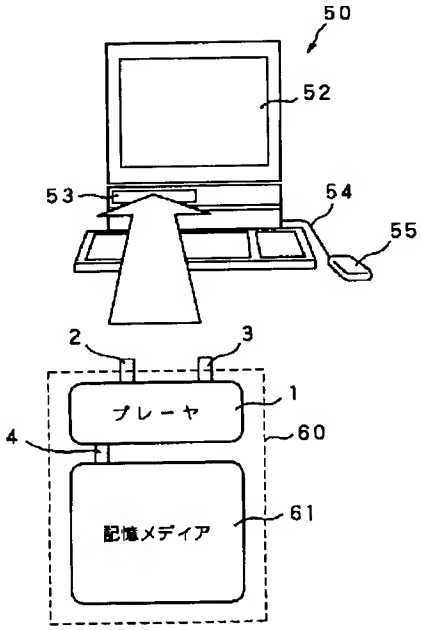
【図３５】



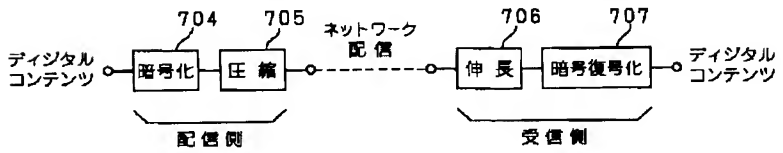
【図２９】



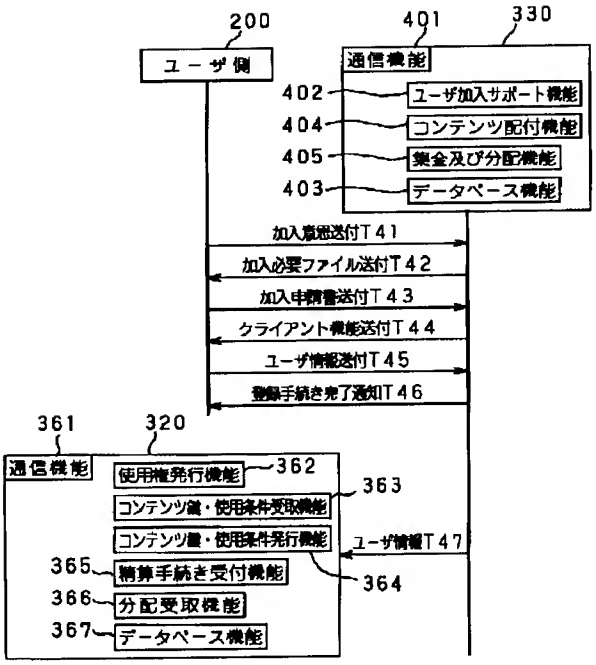
【図３９】



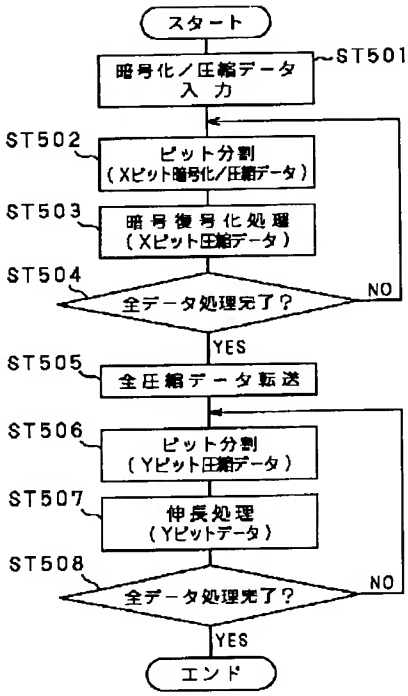
【図４３】



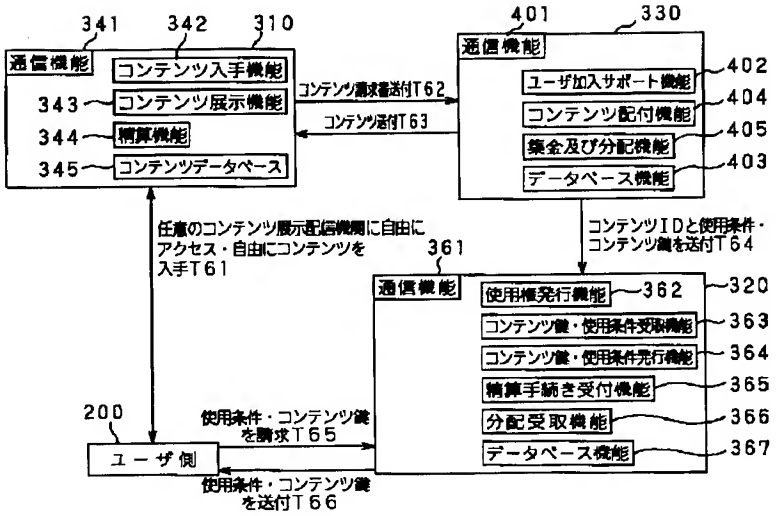
【図３１】


200
401
330
ユーザ側
通信機能
402
ユーザ加入サポート機能
404
コンテンツ配付機能
405
集金及び分配機能
403
データベース機能
加入意思送付T41
加入必要ファイル送付T42
加入申請書送付T43
クライアント機能送付T44
ユーザ情報送付T45
登録手続き完了通知T46
361
320
通信機能
使用権発行機能
362
363
コンテンツ鍵・使用条件受取機能
コンテンツ鍵・使用条件発行機能
ユーザ情報T47
364
365
精算手続き受付機能
366
分配受取機能
367
データベース機能

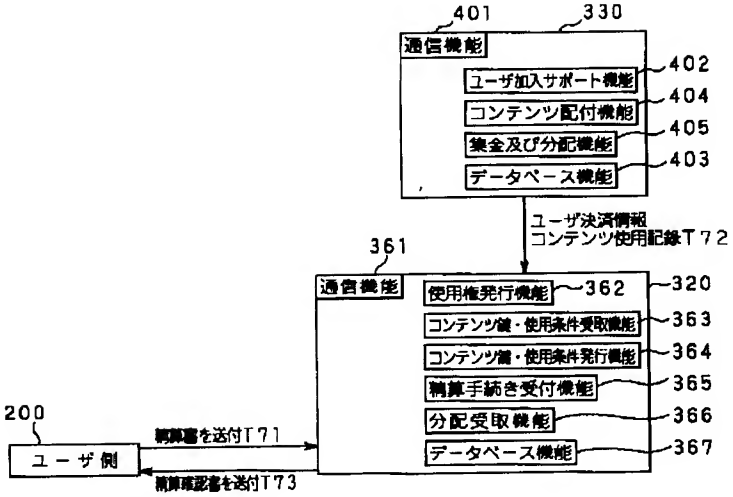
【図４２】


スタート
暗号化ノ圧縮データ入力
ST501
ST502
ビット分割（Xビット暗号化/圧縮データ）
ST503
暗号復号化処理（Xビット圧縮データ）
ST504
全データ処理完了？
NO
YES
ST505
全圧縮データ転送
ST506
ビット分割（Yビット圧縮データ）
ST507
伸長処理（Yビットデータ）
ST508
全データ処理完了？
NO
YES
エンド

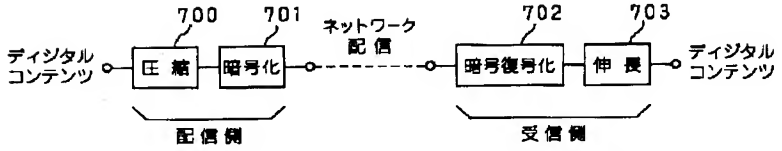
【図３３】


341
342
310
401
330
通信機能
コンテンツ入手機能
コンテンツ展示機能
精算機能
コンテンツデータベース
通信機能
ユーザ加入サポート機能
コンテンツ配付機能
集金及び分配機能
データベース機能
402
404
405
403
コンテンツ請求書送付T62
コンテンツ送付T63
任意のコンテンツ展示配信機関に自由にアクセス・自由にコンテンツを入手T61
コンテンツIDと使用条件・コンテンツ鍵を送付T64
361
通信機能
使用権発行機能
362
320
コンテンツ鍵・使用条件受取機能
363
コンテンツ鍵・使用条件発行機能
364
精算手続き受付機能
365
分配受取機能
366
データベース機能
367
200
ユーザ側
使用条件・コンテンツ鍵を請求T65
使用条件・コンテンツ鍵を送付T66

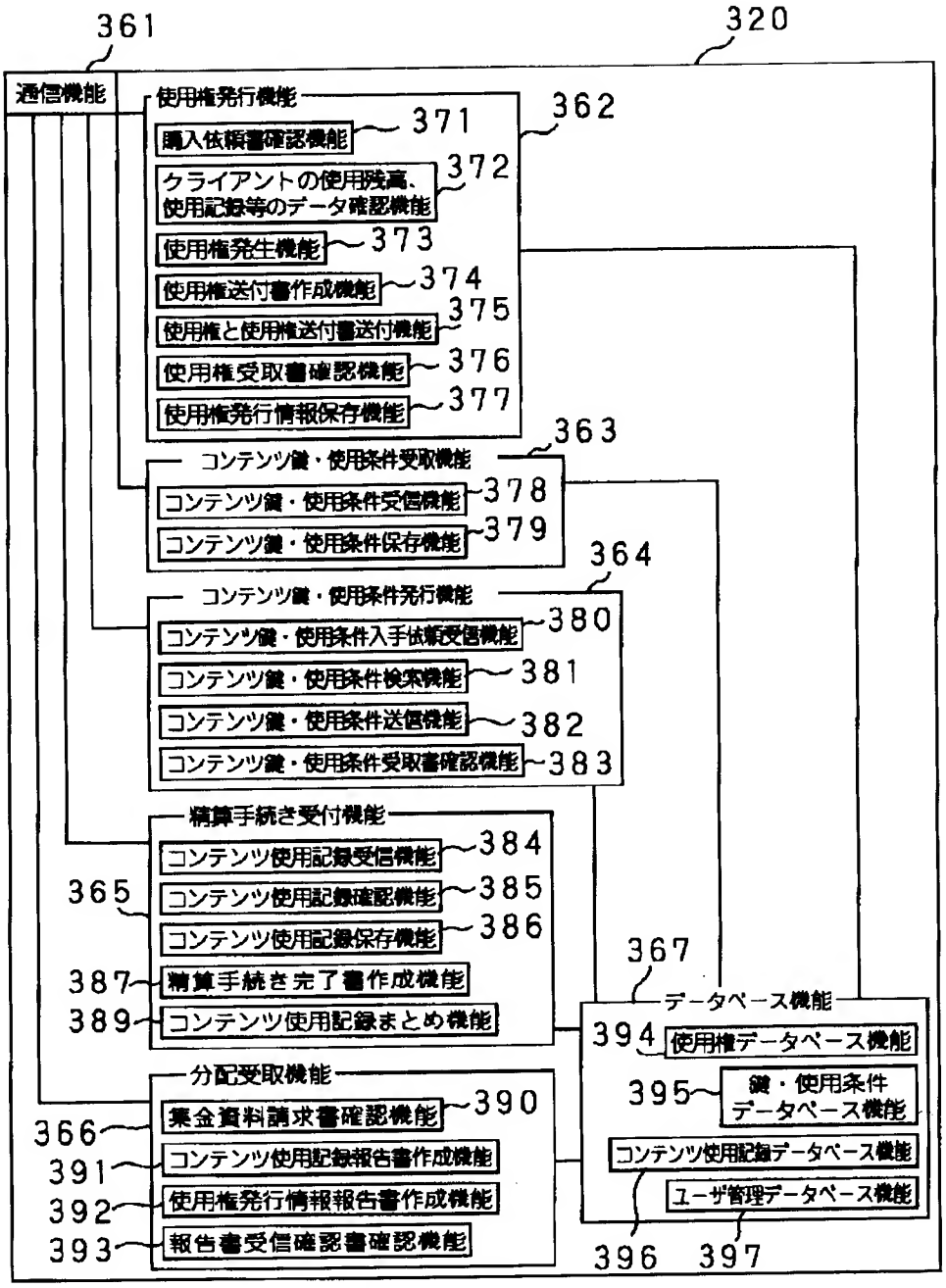
【図３４】


401
330
通信機能
402
ユーザ加入サポート機能
404
コンテンツ配付機能
405
集金及び分配機能
403
データベース機能
ユーザ決済情報
コンテンツ使用記録T72
361
通信機能
使用権発行機能
362
320
コンテンツ鍵・使用条件受取機能
363
コンテンツ鍵・使用条件発行機能
364
精算手続き受付機能
365
分配受取機能
366
データベース機能
367
200
ユーザ側
精算書を送付T71
精算確認書を送付T73

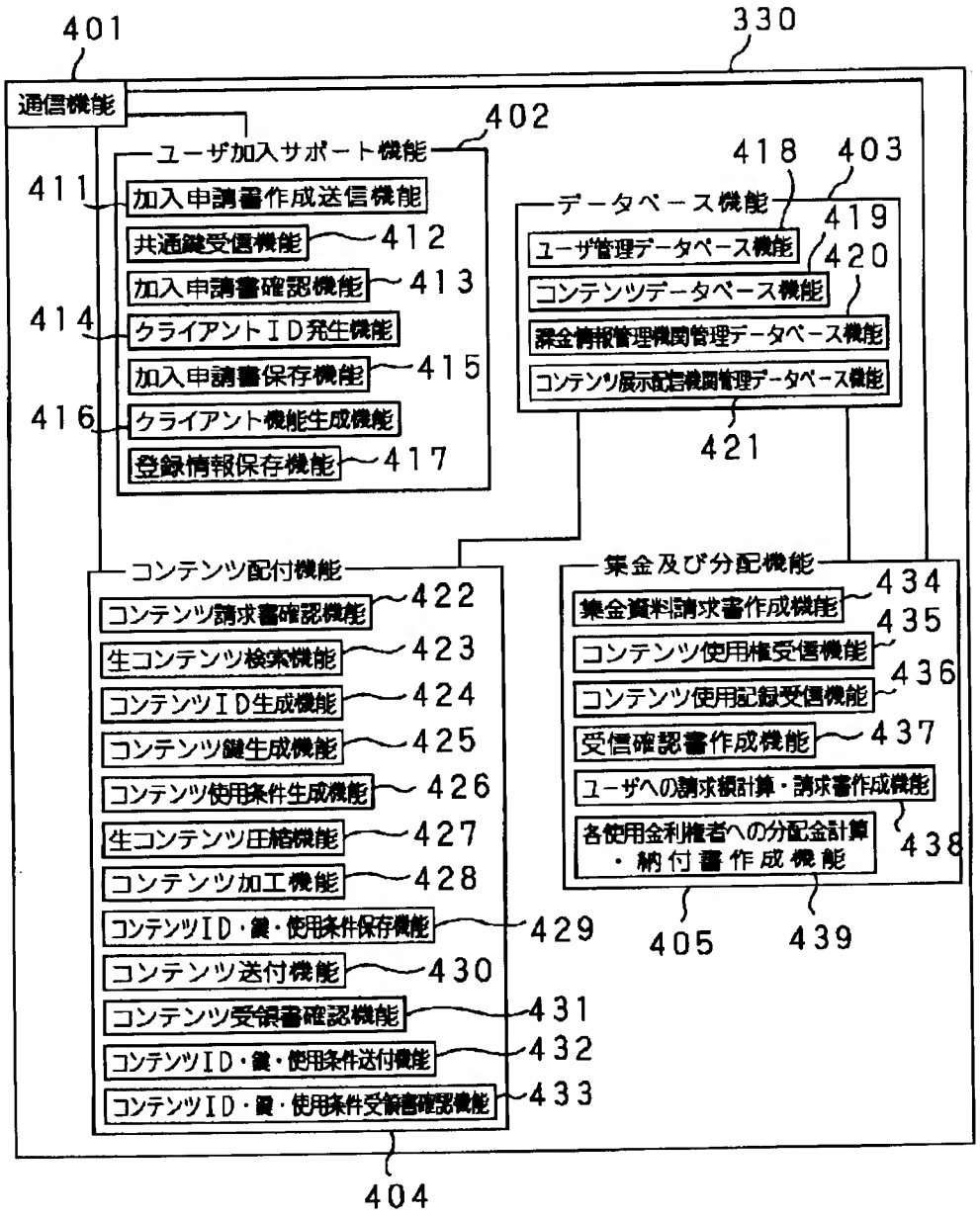
【図４１】


700
701
ネットワーク
配信
702
703
ディジタル
コンテンツ
圧縮
暗号化
暗号復号化
伸長
ディジタル
コンテンツ
配信側
受信側

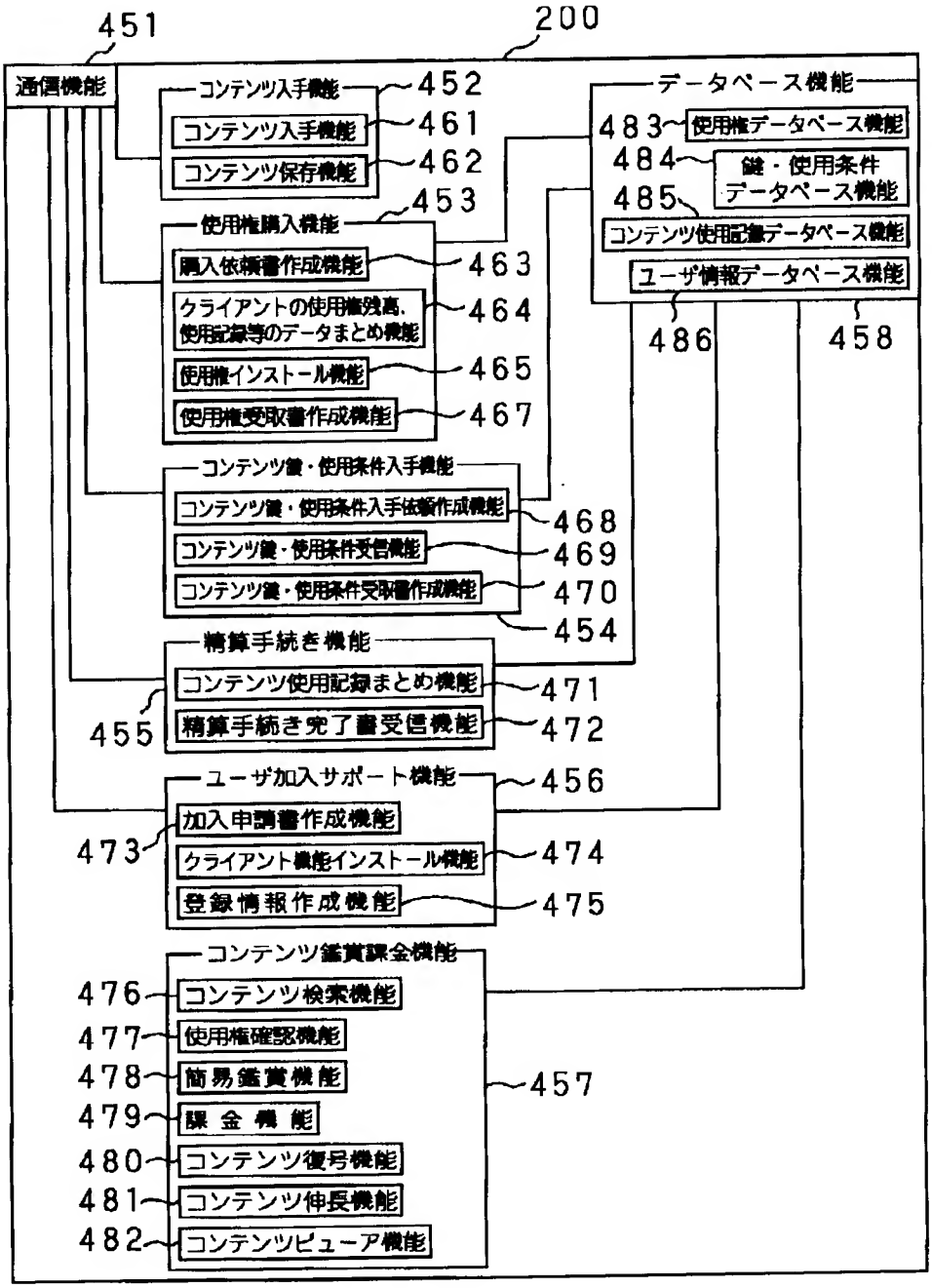
【図３６】


361
320
通信機能
使用権発行機能
362
購入依頼書確認機能
371
クライアントの使用残高、使用記録等のデータ確認機能
372
使用権発生機能
373
使用権送付書作成機能
374
使用権と使用権送付書送付機能
375
使用権受取書確認機能
376
使用権発行情報保存機能
377
コンテンツ鍵・使用条件受取機能
363
コンテンツ鍵・使用条件受信機能
378
コンテンツ鍵・使用条件保存機能
379
コンテンツ鍵・使用条件発行機能
364
コンテンツ鍵・使用条件入手依頼受信機能
380
コンテンツ鍵・使用条件検索機能
381
コンテンツ鍵・使用条件送信機能
382
コンテンツ鍵・使用条件受取書確認機能
383
精算手続き受付機能
365
コンテンツ使用記録受信機能
384
コンテンツ使用記録確認機能
385
コンテンツ使用記録保存機能
386
387
精算手続き完了書作成機能
389
コンテンツ使用記録まとめ機能
分配受取機能
366
集金資料請求書確認機能
390
391
コンテンツ使用記録報告書作成機能
392
使用権発行情報報告書作成機能
393
報告書受信確認書確認機能
367
データベース機能
394
使用権データベース機能
395
鍵・使用条件データベース機能
コンテンツ使用記録データベース機能
ユーザ管理データベース機能
396
397

【図３７】


401
330
通信機能
402
ユーザ加入サポート機能
411
加入申請書作成送信機能
共通鍵受信機能
412
加入申請書確認機能
413
414
クライアントＩＤ発生機能
加入申請書保存機能
415
416
クライアント機能生成機能
登録情報保存機能
417
418
403
データベース機能
419
ユーザ管理データベース機能
420
コンテンツデータベース機能
課金情報管理機関管理データベース機能
コンテンツ展示配信機関管理データベース機能
421
コンテンツ配付機能
422
コンテンツ請求書確認機能
423
生コンテンツ検索機能
424
コンテンツＩＤ生成機能
425
コンテンツ鍵生成機能
426
コンテンツ使用条件生成機能
427
生コンテンツ圧縮機能
428
コンテンツ加工機能
429
コンテンツＩＤ・鍵・使用条件保存機能
430
コンテンツ送付機能
431
コンテンツ受領書確認機能
432
コンテンツＩＤ・鍵・使用条件送付機能
433
コンテンツＩＤ・鍵・使用条件受領書確認機能
404
集金及び分配機能
434
集金資料請求書作成機能
435
コンテンツ使用権受信機能
436
コンテンツ使用記録受信機能
437
受信確認書作成機能
ユーザへの請求額計算・請求書作成機能
各使用金利権者への分配金計算・納付書作成機能
438
405
439

【図３８】


451
200
通信機能
コンテンツ入手機能
452
コンテンツ入手機能
461
コンテンツ保存機能
462
使用権購入機能
453
購入依頼書作成機能
463
クライアントの使用権残高、使用記録等のデータまとめ機能
464
使用権インストール機能
465
使用権受取書作成機能
467
コンテンツ鍵・使用条件入手機能
コンテンツ鍵・使用条件入手依頼作成機能
468
コンテンツ鍵・使用条件受信機能
469
コンテンツ鍵・使用条件受取書作成機能
470
454
精算手続き機能
コンテンツ使用記録まとめ機能
471
455
精算手続き完了書受信機能
472
ユーザ加入サポート機能
456
加入申請書作成機能
473
クライアント機能インストール機能
474
登録情報作成機能
475
コンテンツ鑑賞課金機能
476
コンテンツ検索機能
477
使用権確認機能
478
簡易鑑賞機能
479
課金機能
480
コンテンツ復号機能
481
コンテンツ伸長機能
482
コンテンツビューア機能
457
データベース機能
483
使用権データベース機能
484
鍵・使用条件データベース機能
485
コンテンツ使用記録データベース機能
ユーザ情報データベース機能
486
458